In the High Court of New Zealand
Wellington Registry
I Te Kōti Matua o Aotearoa
Te Rohe o Te Whanganui-ā-Tara

CIV-2025-485-487

under:	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 an application concerning **Cryptopia Limited (in liquidation)** and Cryptopia NZDT Limited (in liquidation)
and	
in the matter of:	an application by **David Ian Ruscoe and Malcolm Russell Moore** as liquidators of Cryptopia Limited (in liquidation) and Cryptopia NZDT Limited (in liquidation) *Applicants*

GNY.io Limited synopsis of submissions for hearing

Dated: 11 May 2026

Judicial Officer: Isac J

REFERENCE: L L Fraser (laura.fraser@chapmantripp.com)
J Marcetic (janko.marcetic@chapmantripp.com)
COUNSEL: Daniel Kalderimis KC (daniel.kalderimis@chambers.co.nz)

chapmantripp.com
T +64 9 357 9000
F +64 4 472 7111

PO Box 2206
Auckland 1140
New Zealand

Auckland
Wellington
Christchurch

chapman tripp

SECTION 1: INTRODUCTION

1 GNY.io Limited (**GNY**) was the developer of the Lisk Machine Learning (**LML**) cryptocurrency token. After careful consideration as to where it should trade that token, GNY paid a listing fee and listed its LML tokens on the exchange platform of Cryptopia; then the world's fourth-largest cryptocurrency exchange.

2 In accordance with Cryptopia's requirements, GNY traded its LML via user accounts: [redacted].

3 In the 14 January 2019 hack of Cryptopia's platform (the **Hack**), GNY lost all of the LML tokens it held on Cryptopia, to the value of approximately 491 Bitcoin. The Hack has been devastating for the LML token and GNY's business generally: the stolen LML tokens were never recovered, and LML consequently suffered an irrecoverable collapse in value.

4 In April 2019, GNY issued proceedings against Cryptopia. Mere weeks later, Cryptopia was placed into liquidation. That liquidation has been, by any measure, highly unusual for New Zealand. In part, this is because of the circumstances of the Hack, and relative novelty of cryptocurrency itself. In part, it is because of Cryptopia's overall surplus of assets over liabilities. The combination of these factors raises important questions for the Court.

5 Cryptopia's accounts contained substantial cryptocurrency assets, which have appreciated in value considerably over time. Many Cryptopia account holders who did not lose all of their assets in the Hack have had valuable assets returned to them. Even so – and despite a substantial (years-long) process to advertise, and return, assets to account holders – it is apparent that there will be a substantial (and valuable) amount of unclaimed crypto-currency assets from solvent Cryptopia accounts.

6 Meanwhile, Cryptopia account holders whose tokens *were* stolen completely by the Hack have yet to have their claims resolved. Absent the availability of unclaimed cryptocurrency assets to meet their claims, they are unlikely to receive any assets or payments from Cryptopia's liquidation. GNY is likely to be the largest Hack

victim: its position is, however, reflective of many other account holders who were victims of the Cryptopia Hack.

7 In July 2019, GNY submitted its creditor claim to the Liquidators. It has had substantial engagement with the Liquidators on its claim over the course of the subsequent seven years. While the Liquidators have provisionally admitted GNY's claim in the liquidation, GNY's claim is yet to be quantified and determined.

8 In March 2025, GNY filed an application requiring confirmation of its creditor claim under the Companies Act 1993. That application was stayed by consent of GNY and the Liquidators, in order for GNY's claim to be determined in the course of the present (omnibus) proceeding brought by the Liquidators.

9 As detailed in these submissions and its supporting evidence, GNY seeks to have its claim fully and finally resolved. GNY also supports orders which would make unclaimed cryptocurrency assets available to Cryptopia's unpaid creditors – in the alternative to paying those assets away to the New Zealand Crown, leaving Cryptopia's creditors without recourse. The Liquidators' evidence confirms that, if the unclaimed assets are available to creditors "the Company's creditors would likely be paid out in full".[1]

10 In advancing its case, GNY takes positions which are, by extension, for the benefit of Hack victims as a whole. It does so against the background of the Liquidators' decision to present the contrary case to Hack victims on every issue. This leaves GNY to be the contradictor, presenting the perspective and interests of Hack victims generally. This perspective is important and deserves serious consideration.

[1] Ruscoe I, 31 July 2025, at [152]; [**201.0023**] at [**201.0063**].

SECTION 2: OVERVIEW

Structure

11 GNY has adopted a different structure for its submissions as compared to the Liquidators.

12 It includes in **Schedule 1** an updated summary of the issues for determination, cross-referenced to the Liquidators' application, GNY's notice of opposition, and both parties' sets of submissions.

13 At a high level, GNY's submissions follow the following structure:

13.1 **Section 3: Key background**.

13.2 **Section 4: GNY's Cryptopia accounts**. GNY addresses this as a preliminary matter: it says the evidence clearly establishes that the two accounts it operated and traded were GNY accounts, not personal accounts of its directors and founders.

13.3 **Section 5**: **Cryptopia's cybersecurity failures & the Hack**. GNY sets out in this section the essential basis for Cryptopia's breaches of duty to Hack victims like GNY, and why those breaches led to the success of the Hack. This analysis provides relevant context for Hack victim claims generally.

13.4 **Section 6: Cryptopia's liability to GNY**. In section 6, GNY addresses Cryptopia's breaches of fiduciary, statutory, contractual and tortious duties to GNY and other Hack victims.

13.5 **Section 7: Cryptopia's "exclusion clauses"**. GNY here addresses and refutes Cryptopia's bold attempt to fully exclude all liability to all account holders. Unlike the Liquidators, GNY does not see this as a threshold question. The exclusion clauses are irrelevant to several of GNY's claims by virtue of the source of Cryptopia's obligation (which cannot be contracted out of); they are irrelevant to the balance of GNY's claims because they are ineffective when tested against the law concerning onerous exclusion clauses.

13.6 **Section 8: Valuing GNY's claim in BTC, not NZD**. This section addresses why it is legally appropriate to measure (and pay) GNY's claim in BTC, not NZD.

13.7 **Section 9: The Value of GNY's claim**. In section 9, GNY calculates the value of its claim, as assessed by its expert evidence.

13.8 **Section 10: Distribution of Surplus Assets**. Section 10 addresses why (and how) the unclaimed trust assets should be made available to Cryptopia's creditors, including Hack victims, rather than paid to the New Zealand Crown.

13.9 **Section 11: Additional Matters**. Section 11 addresses miscellaneous matters raised in the Directions Application.

14 GNY has adduced affidavit evidence from four witnesses:

14.1 [redacted] a [redacted];

14.2 [redacted], a [redacted];

14.3 Mr Dicks, an experienced cybersecurity expert, who offers expert opinion evidence on Cryptopia's cybersecurity state; and

14.4 Mr O'Shea, an experienced valuer, who provides an expert valuation opinion on the value of GNY's claim.

Approach to determining creditor claims

15 The standard of proof in respect of a creditor claim is the balance of probabilities. When a liquidator is considering a creditor's claim, their role is quasi-judicial: liquidators are required to uphold the standards adhered to by judges.[2] A liquidator:[3]

> assesses whether on the information provided the creditor has shown an enforceable claim. The liquidator is required to act objectively, bearing in mind both the interests of the claimant and also the general body of creditors.

---

2 *McPherson's Law of Company Liquidation* (online ed, Thomson Reuters) at [8.500]; *Shed4 Trading Company Ltd v Sanson* [2020] NZHC 2363 at [21].

3 *Shed4 Trading Company Ltd v Sanson* [2020] NZHC 2363 at [21], citing *Tanning Research Laboratories Inc v O'Brien* (1990) 169 CLR 332 at 341.

16 The High Court has confirmed that, because a creditor claim has to be legally enforceable, it has to be proved by evidence admissible in a court of law: "[c]laims cannot be made on the basis of "You can trust us"."[4]

17 In equal measure, the procedure for determining creditor claims is by design not a complete litigation process. As Associate Judge Bell has confirmed, citing McPherson J:[5]

> What is substituted for litigation in the ordinary form is a procedure by which a claimant lodges a verified proof of debt with the liquidator, who admits or rejects it wholly or in part … There can be no doubt that ordinarily such a procedure is, and is designed to be, much more expeditious and less expensive than ordinary proceedings by way of action.

18 Justice McPherson candidly acknowledged that the attainment of perfect justice is, through this process, sometimes sacrificed to expedience.[6] These pragmatic parameters must be borne in mind.

19 Although GNY is required to establish its claim on the balance of probabilities, GNY does not have access to the same information as it would otherwise obtain in Court litigation, including from Cryptopia itself – whose directors and officers are conspicuously absent from this proceeding. The Liquidators' position has been to put GNY to proof on every conceivable point; and GNY has had to advance its claims against Cryptopia in the absence of fulsome discovery, evidence and interrogatories from Cryptopia itself.

20 Even so, GNY's case is that it has done more than what is or should be necessary to establish its claim in this proceeding. GNY has provided fulsome details of its claim, including through responses to the Liquidators' various information requests over the years. GNY has been forthcoming in providing the information available to it (even though much of the relevant information is in Cryptopia's control). This is far from a situation where GNY is asking the Liquidators, and now the Court, to "just trust us". In this context, the Court may be called upon to consider how to assess any factual gaps that may remain after all the evidence has been considered. GNY records that there may be a case for inferences to be drawn in

---

4 *Shed4 Trading Company Ltd v Sanson* [2020] NZHC 2363 at [22].
5 *Vlasic v Zelande Ltd* [2019] NZHC 2152, citing *Re Gordon Grant & Grant Pty Ltd* [1983] 2 Qd 314 at 316–7.
6 *Vlasic v Zelande Ltd* [2019] NZHC 2152, citing *Re Gordon Grant & Grant Pty Ltd* [1983] 2 Qd 314 at 316–7.

respect of relevant and material information that has been sought from Cryptopia, but not provided by the Liquidators.

SECTION 3: KEY EVENTS

21 Before turning to the key matters in dispute, GNY sets out below relevant background matters to its position on the Liquidators' application. GNY does not repeat the more extensive explanation of background matters provided in the affidavits of [redacted].

GNY.io Limited

22 GNY was established in 2018. It developed the world's first decentralised machine learning platform. As a company GNY harnesses blockchain technology to deliver AI tools for the cryptocurrency community, and tools for AI networks to back up any learning data.

23 GNY is the developer of both the GNY tokens and the LML token. It first listed the LML token on the Cryptopia exchange in 2018. Nearly all of the LML on the exchange was stolen in the Hack in 2019 – with devastating effects for LML and GNY.

GNY & Cryptopia

24 GNY's claim relates to events before Cryptopia's liquidation. The key events are summarised in the course of these submissions where relevant, and in the **Chronology** attached as **Schedule 2.**

25 The key background matters relevant to GNY's claims against Cryptopia are:

25.1 Cryptopia's engagement with GNY in 2018, leading to the listing of the LML token on the Cryptopia platform, and the trading of that token. This is explained in **Section 4**, including explaining that GNY worked with Cryptopia to open its trading accounts in its own name for the purpose of listing the LML token – and that GNY took this step on the basis of assurances from Cryptopia that its platform was "safe" and "secure".[7]

25.2 Cryptopia's very poor cybersecurity state over the course of 2017 and 2018. This is explained in **Section 5**. Cryptopia

[7] GNY's reliance on these assurances is detailed in Section 6.

repeatedly failed basic penetration testing of its platform: its cybersecurity advisors were able to secure unrestricted access to Cryptopia's wallet environment (where valuable cryptocurrency was stored) undetected and unimpeded by any effective security defence. In one "catastrophic"[8] instance, the attackers gained full control over all of Cryptopia's information and systems without detection for three days – using "moderate to low" sophistication hacking techniques.[9] These failures reflected numerous other cybersecurity vulnerabilities raised with Cryptopia by its cybersecurity advisors, Pulse Security. Many of these vulnerabilities were "critical or severe".[10]

25.3 Cryptopia's failure to take steps to address its highly vulnerable cyber-security state over a period of close to 18 months – despite being warned by the GCSB during this period that it was an identified target of international hackers. This is explained in **Section 6**.

26 On 11 April 2019, GNY issued proceedings against Cryptopia in the Christchurch High Court alleging breaches of duty and loss as a result of the Hack.[11] On 14 May 2019, immediately prior to the due date for its statement of defence, Cryptopia was placed into liquidation. GNY's High Court proceeding was automatically stayed.

The Liquidators provisionally admit GNY's creditor claim

27 On 10 July 2019, GNY submitted its creditor claim form to the Liquidators.[12] GNY's creditor claim explained its loss arising from the lost LML tokens that were stolen in the Hack, and the lost market capitalisation as a result. The extent of GNY's loss and accordingly the valuation of its claim is addressed in **Section 9** below.

28 On 31 July 2020, the Liquidators confirmed their "preliminary assessment is that [GNY] is a creditor of Cryptopia in relation to

---

8 Dicks I, 18 December 2025, at [40.3]; [**201.0154**] at [**201.0167**].
9 Dicks I, 18 December 2025, at [40.3]; [**201.0154**] at [**201.0167**].
10 Dicks I, 18 December 2025, at [12.5]; [**201.0154**] at [**201.0158**].
11 [redacted], 30 March 2025, at [26]; [**201.0001**] at [**201.0006**].
12 [redacted], 30 March 2025, at [28], [**201.0001**] at [**201.0006**]; [redacted]51; [**302.0949**].

account holder losses and it is working through issues associated with the quantum of the claim to be admitted".[13]

29 GNY has therefore been recorded as a "contingent creditor" in the Liquidators' reports for coming up to six years now.[14] However, there has been no final confirmation of GNY's claim, including ascertainment of the amount. That is one important purpose of this proceeding.

The Court's Trust Decision (Gendall J)

30 GNY was not heard on the Liquidators' 2020 directions application leading to a High Court decision which determined that Cryptopia held the cryptocurrencies, which were determined to be property, on express trusts for the benefit of account holders, and that a separate trust existed in respect of each Cryptocurrency (the **Trusts**).[15]

31 On 10 July 2019, GNY advised the Liquidators that it anticipated that matters relating to asset distribution and the conduct of the liquidation would require significant direction from the New Zealand courts, and that it may wish to be heard on a number of matters relating to the distribution of crypto assets.[16]

32 On 1 October 2019, the Liquidators commenced a directions application as to the legal status of the cryptocurrencies within Cryptopia's control, and whether the remaining cryptocurrency was held on trust for account holders.[17]

33 The orders for representation and service of that application were made without the Court being made aware of GNY's claim in the liquidation as a Hack victim (or of any circumstances that may be relevant to Hack victims generally). The Liquidators' application included the following description of creditor claims:[18]

---

13 [redacted] 30 March 2025, [redacted]104; [**201.0001**] at [**303.1034**].
14 For example, [redacted] 30 March 2025, [redacted] 156 – 171; [**201.0001**] at [**303.1141**] - [**303.1157**].
15 *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728, [2020] 2 NZLR 809 at [133], [183], [187], [196] and [209]; [**401.0365**] at [**401.0413**], [**401.0428**], [**401.0429**], [**401.0431**] and [**401.0436**].
16 [redacted] 30 March 2025, [redacted]52; [**201.0001**] at [**302.0950**].
17 Originating application by Liquidators for directions in relation to digital assets held by the company, dated 1 October 2019. [**401.0187**]
18 Interlocutory application for orders as to representation and directions as to service, 1 October 2019, para 2(d)(ii); [**401.0187**] at [**401.0190**]

> There are 37 known unsecured creditors with claims valued at NZD12.7 million who will have an interest in the Originating Application, as persons who may receive a distribution as creditors of Cryptopia. There may be additional creditors, who are not yet known to the Liquidators, such as parties who may have a claim against Cryptopia.

34 GNY's claim alone (submitted to the Liquidators some months prior) exceeded these indicative figures. While accountholders were notified by email that the Liquidators had sought directions from the Court, GNY was represented by counsel on their creditor claim, who were not advised.[19]

35 The Court therefore made findings on the directions application without hearing from Hack victims like GNY. GNY had no appeal rights with respect to that decision.

36 While GNY accepts the decision is binding on it insofar as it holds that Cryptopia held assets in its trading accounts as a bare trustee, and that those assets are property (the **Trust Decision**),[20] it does not accept the Liquidators' position that the Trust Decision is dispositive of a range of other points which are before the Court in the present directions application, but which were not actually argued in the directions application, and which were not before the Court for determination in the Trust Decision.[21] In particular, GNY does not regard the Trust Decision to somehow preclude the principled and practical use of surplus assets to satisfy unpaid Hack victims.

GNY's March 2025 application

37 In December 2024, when the hard cut-off date for accountholder claims had been reached, GNY wrote to the Liquidators to again ask

---

19 On 1 October 2019, the Liquidators filed the Directions Application, including the Interlocutory Application for Orders as to Representation and Directors as to Service [**401.0187**]. Those orders were determined on 14 October, and sealed orders issued on 18 October. On 25 October 2019, the Liquidators made the claim material available publicly on their website: see affidavit of David Ruscoe in support of Originating Application for Orders for Directions Regarding the Distribution of Digital Assets dated 31 July 2023, DIR1-188; [**301.0282**] at [**301.0288**]. On 4 November 2019, Cryptopia stakeholders were sent an email with a link to the Liquidators' 25 October 2019 update. The Directions Application was heard on 3-4 February 2020.

20 *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728, [2020] 2 NZLR 809 at [133], [183], [196] and [209]; [**401.0365**] at [**401.0413**], [**401.0428**], [**401.0431**] and [**401.0436**].

21 Liquidators' Submissions, [6.5].

the Liquidators to finally accept its creditor claim in whole, including as to quantum.[22]

38 GNY confirmed its claim against Cryptopia should account for developments in the Liquidation in the six years since its claim was submitted, including the Trust Decision establishing Cryptopia's obligations to accountholders as a trustee.[23]

39 The Liquidators did not confirm GNY's claim. After over six years without progress to resolve its entitlements, GNY filed an application for orders requiring confirmation of its claim under the Companies Act in March 2025.[24]

40 GNY and the Liquidators ultimately agreed that GNY's creditor claim would be determined in the course of this proceeding.

Confidentiality & provision of information

41 Obtaining access to some information relevant to this proceeding has been challenging for GNY. At the same time, the Liquidators have not protected its confidential information.

Relevant information withheld

42 The Liquidators have declined to make available transcripts of s 261 interviews they undertook with Cryptopia's directors and senior managers on matters concerning Cryptopia's cybersecurity protections, despite this issue being of central relevance to the legal claims of Hack victims including GNY.[25]

43 More recently, the Liquidators have sought confidentiality orders over even aggregated information about the value of Cryptopia's unclaimed holdings. None of the reasons for seeking confidentiality over that material apply to GNY: it is not a "malefactor[s] known to the liquidators and this Court"[26] and it is not clear on what basis the Liquidators apprehend any real risk that disclosing those (static)

---

22 [redacted] 30 March 2025, [redacted]121; [**201.0001**] at [**303.1351**].

23 [redacted]s not a newly ado[redacted]position: GNY had also written to the Liquidators confirming Cryptopia's obligations to account holders as trustees following release of the Trust Decision: See also GNY's 12 May 2020 letter at [redacted] 30 March 2025, [redacted]84; [**201.0001**] at [**303.1012**].

24 [redacted]locutory application on notice for orders requiring confirmation of creditor claim under the Companies act 1993, dated 31 March 2025; [**401.0540].**

25 See discussion at [**166**] below.

26 Liquidators' Memorandum of Counsel, 23 April 2026, at [3]; [**401.0157**] at [**401.0158**].

holdings could "result in market manipulation about those holdings".[27] Earlier in the proceeding, when the parties exchanged GNY's confidential and commercially sensitive material, that has occurred on the basis of undertakings. It is not clear why that practice could not have continued with respect to the value of Cryptopia's unclaimed holdings.[28]

44 The withheld information is relevant to further directions in the liquidation. This is why the Liquidators advised the Court that they intended to provide it with updating information about the likely unclaimed holdings at the time the application was filed.[29] It is legally relevant to valuation matters[30] and of obvious importance to Cryptopia creditors and Hack victims – particularly including GNY, given the amount of time, and resources, it is expending to pursue its claim without any clear understanding of the possibility of recovery.

Confidential information made public

45 By contrast, GNY's confidential information has not been treated with care.

46 The Liquidators applied for, and were granted, orders as to service of this proceeding (including evidence filed in it) on Cryptopia accountholders on an ex-parte basis.

47 GNY was not served with this application, nor told of the Court's decision. It should have been, as a party to the proceeding. Further, the Liquidators' evidence contained confidential information about GNY's accounts - and private, identifying information about GNY's two directors and founders.

48 The Liquidators published the Court documents on their website, including Mr Ruscoe's affidavit which contained GNY's confidential and private information. The Liquidators did not redact those

---

27 Liquidators' Memorandum of Counsel, 23 April 2026, at [2]; [**401.0157**] at [**401.0158**].

28 In an earlier proceeding in relation to the Cryptopia liquidation, the Liquidators have provided (on an unredacted basis) aggregate information about Cryptopia's assets based on the Liquidators' initial inquiries, including a conservative estimate of the account holders' holdings: Affidavit of David Ruscoe in support of Origination Application Without Notice for Directions in relation to Digital Assets at [14]; [**401.0576**] at [**401.0579**].

29 Ruscoe I, 31 July 2025, at [150]; [**201.0023**] at [**201.0063**].

30 Discussed further at **Section 9** below.

details. This step disclosed GNY's private information to over a million Cryptopia account holders.

49 When GNY realised what had happened, it raised its concerns with the Liquidators. GNY advised that the information disclosed in Mr Ruscoe's affidavit was private information of beneficiaries which should have been redacted. GNY's view was consistent with the position the Liquidators have adopted about information of this kind in related proceedings.[31] GNY was concerned that disclosure of personal details to over a million accountholders and creditors would pose an harassment risk, particularly as the Liquidators had made their application available publicly, but had withheld GNY's notice of opposition, making the overall disclosure imbalanced. GNY requested that the Liquidators replace Mr Ruscoe's affidavit with a redacted version instead.[32]

50 The Liquidators initially resisted making any change, notwithstanding that in different contexts they had accepted that identifying details of accountholders were private and confidential.[33] Urgent and iterative correspondence was required before the Liquidators eventually agreed to the redactions sought.[34] Even after that agreement was reached, for a further five days an unredacted version of Mr Ruscoe's affidavit remained on the Liquidators' servers, the link in emails sent to creditors and account holders still went to the unredacted affidavit, and the unredacted affidavit could still be found by Google search.[35]

51 From GNY's perspective, it has been challenging to experience its reasonable concerns about privacy and harassment treated with resistance – while at the same time, being refused access to information relevant to its creditor claim to which, as a responsible participant in this application, it ought to have access.

---

31 *Ruscoe v Epic Trust Ltd* [2025] NZHC 2138 at [57].
32 Alcartado I, 7 May 2026, PA1-38 – 40; [**401.0589**] at [**401.0629**] - [**401.0631**].
33 *Ruscoe v Epic Trust Ltd* [2025] NZHC 2138 at [57].
34 Alcartado I, 7 May 2026, PA1-41 – 27; [**401.0589**] at [**401.0618**].
35 Alcartado I, 7 May 2026, PA1-41; [**401.0589**] at [**401.0632**].

SECTION 4: GNY'S CRYPTOPIA ACCOUNTS

52 GNY held two Cryptopia trading accounts.

53 GNY's listing of its LML token on the Cryptopia platform occurred through two user accounts. The usernames for the two accounts were [redacted] and [redacted]. The accounts were operated by [redacted], [redacted] and [redacted] respectively, and were linked to their email accounts.[36] LML was first placed into those accounts pursuant to GNY's listing arrangements with Cryptopia, and was initially traded from those accounts.

54 The Liquidators have suggested that they may not be required to admit GNY's claim because GNY was not a Cryptopia account holder – apparently on the basis that Cryptopia's Terms and Conditions did not permit Cryptopia accountholders to transact on behalf of a third party, nor allow one person to hold multiple accounts.[37] In their submissions, the Liquidators have also suggested (for the first time, and contrary to their own evidence) that Cryptopia did not know that the two accounts were GNY accounts.[38] The Liquidators' objections are both technical and wrong, although it does illustrate the extent the Liquidators have chosen to go to in opposing GNY's claim.

GNY's accounts are GNY's accounts

55 Cryptopia always understood – and accepted – that the [redacted] and [redacted] accounts were GNY accounts.

56 The relevant correspondence between GNY and Cryptopia is very clear on this issue:[39]

56.1 in October 2018, GNY approached Cryptopia about listing LML on the platform.[40] Specifically, on 15 October 2028, [redacted]

---

36 Ruscoe I, 31 July 2025, at [56]; [**201.0023**] at [**201.0039**].
37 Ruscoe I, 31 July 2025, at [11] and [57]; [**201.0023**] at [**201.0026**] and [**201.0039**].
38 Liquidators' Submissions, [8.40].
39 Sibenik I, 1 August 2025, PJS1-79 – 91; [**201.0090**], [**302.0799**]–[**302.0811**].
40 Sibenik I, 1 August 2025, PJS1-15; [**201.0090**], [**302.0718**].

approached Cryptopia expressly on behalf of GNY, and as the [redacted];[41]

56.2 Cryptopia required GNY to complete a listing information form and go through a series of verification and review steps, before LML could be listed.[42] That form was express that the "Legal Entity which oversees the [LML listing] project" was "GNY IO", an entity registered in Jersey. Cryptopia required GNY to attach its certificate of incorporation to that listing form. GNY completed the listing form expressly on the basis that "GNY IO the company are issuing the token". The form also made clear that [redacted] existing [redacted] account would be used for GNY's listing of LML, and nominated [redacted] as an "additional team member you would like to participate in your [that is, GNY's] coin listing", while explaining to Cryptopia that [redacted]

56.3 following GNY's provision of listing information to Cryptopia, Cryptopia's project review team undertook a review of that information. This took approximately 15 days and, as per the information requested on the Listing Form, included reviewing detailed GNY business plans, KYC information, GNY's two key project team members, [redacted] and [redacted] existing Cryptopia account;[43]

56.4 on 5 November 2018, Cryptopia advised [redacted] that GNY's proposal had "passed our project review and is ready to progress".[44] Cryptopia was well aware by this point that the proposed LML listing was a GNY project, and that [redacted] and [redacted] were [redacted] as well as the two identified GNY key contacts for GNY's LML listing on the Cryptopia platform;

56.5 on 5 November 2018, in the course of GNY's listing process, Cryptopia provided GNY with its Listing Contract for the LML project, setting out the terms and pricing options for the

41 Sibenik I, 1 August 2025, PJS1-9; [**201.0090**], [**302.0719**] at [**302.0720**].
42 Sibenik I, 1 August 2025, PJS1-8; [**201.0090**], [**302.0719**].
43 Sibenik I, 1 August 2025, PJS1-21 – 22; [**201.0090**], [**302.0732**] at [**302.0733**] –[**302.0734**].
44 Sibenik I, 1 August 2025, PJS1-20; [**201.0090**], [**302.0732**].

listing.[45] [redacted] confirmed GNY was happy to accept the quote in that contract on the same day;[46]

56.6 as a KYC requirement for the listing, Cryptopia required GNY to ensure that a key contact of the GNY team was registered on the exchange and appropriately verified to "level 2".[47] At that time [redacted] already had a registered Cryptopia account under the username [redacted] Cryptopia expressly confirmed to [redacted] that his existing account met Cryptopia's KYC requirements for listing purposes;[48]

56.7 GNY paid the Listing Quote listing fee by purchasing the required 3.3m DOT through the [redacted] account and transferring the fee to Cryptopia, as required.[49] Cryptopia confirmed receipt of payment.[50] Cryptopia then proceeded to code review and built the environments necessary for GNY's LML listing – an LML wallet, and LML information and trading details pages. This took several weeks; and

56.8 [redacted] opened a Cryptopia account as the second team member nominated to participate in GNY's LML listing. Once Cryptopia confirmed that its coding work was complete,[51] LML was then listed on the exchange via the [redacted] and [redacted] accounts.[52]

57 Cryptopia therefore knew that it was dealing with GNY throughout.

58 It is also clear that:

58.1 all of GNY's communications were with the same Cryptopia listing analyst. Cryptopia understood from these communications that GNY was planning to list the LML token, and [redacted] and [redacted] were GNY officers;

---

45 [redacted] I, 30 March 2025, [redacted]; [**201.0001**], [**302.0731**].
46 [redacted] 1, 1 August 2025, PJS1-28; [**201.0090**], [**302.0745**] at [**302.0748**].
47 Sibenik I, 1 August 2025, PJS1-18; [**201.0090**], [**302.0737**] at [**302.0739**].
48 Sibenik I, 1 August 2025, PJS1-28; [**201.0090**], [**302.0745**] at [**302.0748**].
49 Sibenik I, 1 August 2025, PJS1-26; [**201.0090**], [**302.0745**] at [**302.0746**].
50 Sibenik I, 1 August 2025, PJS1-25; [**201.0090**], [**302.0745**].
51 Sibenik I, 1 August 2025, PJS1-26; [**201.0090**], [**302.0745**] at [**302.0746**].
52 See generally, [redacted] 19 December 2025; [**201.0141**].

58.2 Cryptopia required GNY to hold a Level 2 verified trading account in order to list LML on the Cryptopia platform;[53]

58.3 to open an account, practically, a user needed to create a username, and password, and nominate a specific email address.[54] By their nature, usernames and passwords are individual, and email addresses typically belong to natural persons. This is why the two GNY accounts are linked to [redacted] respective email addresses. This is the only way that a corporate entity could open a trading account on the Cryptopia platform. And, stating the obvious, listing a coin required that coin to be made available to traders via a trading account;

58.4 at no stage did Cryptopia suggest to GNY in their communications concerning the planned listing of LML on the exchange that it could not operate two accounts for its LML listing project. In fact, Cryptopia's Listing Form anticipated at least two team members would participate in the coin listing. And GNY explicitly provided Cryptopia with the identities of the two team members it expected to participate in the LML listing project: [redacted];[55] and

58.5 at no stage during GNY's listing engagement with Cryptopia did Cryptopia suggest that GNY could not open its trading accounts using details of natural persons, such as email addresses and personal usernames / passwords. As noted above, practically speaking, the only way GNY could actually open an account was using individual details of this kind. Against this background, Cryptopia positively affirmed in writing to GNY that the use of [redacted] existing account using his individual details was suitable for satisfying Cryptopia's listing requirement that GNY have a KYC level 2 verified account.[56]

---

53 See the Listing Form: Sibenik I, 1 August 2025, PJS1-8; [**201.0090**], [**302.0719**].
54 Brocket I, 27 November 2019, TJSB1-39 – 41; [**401.0194**] at [**401.0239**] - [**401.0241**].
55 Sibenik I, 1 August 2025, PJS1-8; [**201.0090**], [**302.0719**].
56 Sibenik I, 1 August 2025, PJS1-28; [**201.0090**], [**302.0745**] at [**302.0748**].

59 It is therefore surprising that the Liquidators have taken the view (in evidence) that "GNY's trust and contractual relationship is with Messer [redacted].[57] The basis for this position appears to be that Cryptopia's account holder Terms and Conditions specified that accounts could not transact on behalf of third parties, and traders could not have multiple accounts.

60 However, Cryptopia did not impose any such legal requirements on GNY. In fact:

60.1 In its Listing Form, Cryptopia suggested that it was expected for multiple team members to participate in a single coin listing. Listing a coin for trading could only occur via trading accounts.

60.2 Cryptopia confirmed to GNY that the account linked to [redacted] was an acceptable account to it for GNY's listing, as it complied with Cryptopia's level 2 KYC requirements.

60.3 Cryptopia did not include these purported requirements in its GNY Listing Form, its GNY Listing Contract, or in its extensive engagement with GNY prior to GNY placing the LML tokens in its two Cryptopia accounts.

60.4 And, as is explained in detail elsewhere in these submissions, Cryptopia's accountholder Terms and Conditions were never actually shown to [redacted] notwithstanding the detailed process GNY went through with Cryptopia to list the LML token for trading.[58]

61 It is not credible for Cryptopia to belatedly suggest that its standard form accountholder Terms and Conditions (which were never brought to GNY's attention at the time of listing LML or at the time of opening its accounts, despite repeated direct engagement with Cryptopia) somehow override the arrangements on which GNY and Cryptopia acted in 2018. The course of conduct between GNY and

---

57 Ruscoe I, 31 July 2025, at [57]; [**201.0023**] at [**201.0039**].
58 See [**276**] – [**289**].

Cryptopia demonstrates the basis of the parties' contractual relationship.[59]

62 The Liquidators' alternative analysis of these events as presented in their submissions is flawed in a number of key respects:

62.1 the Liquidators' submissions analyse the course of correspondence between GNY and Cryptopia (selectively) and suggest that Cryptopia was unaware that the two accounts were operated for GNY.[60] This is quite incorrect. Even apart from all of the direct engagement described above, Cryptopia needed to build a full wallet infrastructure for GNY to launch LML as a new coin on the Cryptopia platform, and LML was placed into the accounts on its launch date.[61] Cryptopia typically posted announcements to Twitter and to its Knowledge Base announcing new LML listings once a listing project confirmed it was ready to launch.[62] Cryptopia knew that the accounts into which LML was placed were accounts operated by GNY for the purpose of GNY listing LML on the Cryptopia exchange;

62.2 the Liquidators suggest that there is "no evidence" of GNY "informing Cryptopia that [redacted] accounts had "become" corporate accounts".[63] This too is incorrect. GNY's Listing Form for LML, completed by [redacted] on GNY's behalf, specifically identified [redacted] existing [redacted] account, linked to his email address [redacted], as his level 2 verified account on Cryptopia.[64] The reason the Listing Form required the identification of any existing account is because Cryptopia required GNY to confirm to had a level 2 verified account

---

59 *BDM Grange Ltd v Trimex Pty Ltd* [2017] NZCA 12, [2017] NZCCLR 11 at [44], see also [7] and [39] to see how the Court used the parties' correspondence and course of conduct to determine what the contract actually meant; *Thompson v Continental Car Services Ltd* [2018] NZHC 1507 at [146]–[147].

60 Liquidators' Submissions, [8.32].

61 See exchanges between Cryptopia and [redacted] confirming GNY's intention to launch LML into the wallet built by Cryptopia for this purpose: Sibenik I, 1 August 2025, PJS1-8 – 91; [**201.0090**], [**302.0719**] – [**302.0811**].

62 See the commitment to do so recorded at Sibenik I, 1 August 2025, PJS1-18; [**201.0090**].

63 Liquidators' Submissions, [8.34].

64 Sibenik I, 1 August 2025, PSJ1-8; [**201.0090**], [**302.0719**].

before agreeing to list LML. This is express in the parties' correspondence. Cryptopia had advised GNY by email that:[65]

> Before your project can proceed through to Code Review, we will need to ensure *a key contact from your team is registered on our exchange, is Level 2 Verified and that they have made a listing payment via our Coin Listings page.*[66]
>
> (emphasis added)

62.3 [redacted] engaged with Cryptopia on these requirements directly by email. Cryptopia passed GNY's proposed LML listing through its 15-day project review process – on the basis that the [redacted] account was the GNY team member level 2 verified account. It then received GNY's listing fee by payment from the [redacted] account, having again liaised with [redacted] on email to ensure that GNY paid that fee in satisfaction of the listing conditions quoted above. Again, Cryptopia knew this was a GNY account;

62.4 as for the Liquidators' suggestion that that [redacted] never advised Cryptopia that his account had "become" a GNY account, that suggestion is based on an incorrect factual premise: [redacted] account was *created* to facilitate the listing of LML, his account was always a GNY account from the outset. GNY's Listing Form makes clear that at the time GNY contacted Cryptopia to establish its trading in LML [redacted] and he would participate in the LML listing as a GNY team member – but he did not yet have a Cryptopia account, so would need to create one;[67]

62.5 the Liquidators also suggest that the Listing Contract was "entirely separate" to GNY's account holder Terms and Conditions and therefore correspondence concerning the Listing Contract "does not assist".[68] This is artificial. GNY listing LML on the exchange and GNY trading LML on the exchange are not separate matters legally, or factually. Legally, as noted above, Cryptopia *required* GNY to hold a verified account on the platform in order to list LML on the

---

65 Sibenik I, 1 August 2025, PSJ1-18; [**201.0090**], [**302.0737**] at [**302.0739**].
66 Sibenik I, 1 August 2025, PSJ1-18; [**201.0090**], [**302.0737**] at [**302.0739**].
67 Sibenik I, 1 August 2025, PSJ1-8; [**201.0090**], [**302.0719**].
68 Liquidators' Submissions, [8.39].

platform. Factually, a successful listing LML could only be achieved in practice by establishing accounts on the exchange into which LML could be placed and then traded from. This is why Cryptopia had account requirements as conditions of listing. It is contrived (and incorrect) to suggest that Cryptopia engaged extensively with GNY about listing LML on the platform, but would somehow not foresee or understand from that engagement that GNY would then actually need to place LML into the trading accounts established by its team members on the exchange so that the token could in fact be traded;

62.6 As the Liquidators properly accept, corporate entities were permitted to open accounts by Cryptopia's Terms and Conditions. But the way a corporate entity could operate an account on the platform was through providing details of natural persons such as email addresses, usernames, and individual passwords. This is what GNY did. The Liquidators' position that "there was no Cryptopia account in GNY's name" ignores the reality that companies have to act through natural persons generally, but particularly in this context where the platform sign up required details associated with natural persons.[69] If the Liquidators' position on this topic is that the accounts cannot be GNY accounts because the username was not "GNY" and the emails used were not "gny.com" or "gny.io" emails,[70] then that suggestion is formalistic and unsustainable given Cryptopia was advised of [redacted] and [redacted] identities, roles with GNY, and roles on the GNY LML listing project, including their proposed participation as nominated team members in GNY's planned LML listing; and

62.7 finally, the Liquidators' suggestion in submissions that there is "no evidence to support the argument that the Accounts became GNY's because Cryptopia acquiesced to that"[71] is not only contradicted by all of the primary material referred to

---

69 Liquidators' Submissions, [8.25].

70 This does appear to be the Liquidators' proposition: see Liquidators' Submissions at [8.26], which relies on the fact the email addresses used were personal email addresses, and the usernames appeared to be personalised to the account operators.

71 Liquidators' Submissions, [8.40].

above – it also ignores the Liquidators' own evidence on this topic. As Mr Ruscoe quite properly accepts in his evidence:[72]

> There is correspondence between Cryptopia's listing team and GNY which indicates that Cryptopia knew that [redacted] and [redacted] accounts were operated on behalf of GNY and did not y objection.

63 It is even more surprising that the Liquidators point to [redacted] and [redacted] completing the Liquidators' claims portal post-liquidation in order to contend that the accounts in question were personal, not GNY, accounts.[73] The Liquidators have not fairly described the background to GNY's engagement with the portal process. Relevantly:

63.1 GNY has engaged with the Liquidators in correspondence since 2019 on the basis that the [redacted] and [redacted] accounts are GNY accounts;[74]

63.2 GNY provided the Liquidators with a creditor claim form well before the Liquidators' accounts portal was opened, in its own name, and expressly in connection with losses connected to its two trading accounts;[75]

63.3 on 31 July 2020, the Liquidators provisionally accepted that GNY is "a creditor of Cryptopia in relation to account holder losses" (subject to quantum);[76]

63.4 the Liquidators communicated this position to GNY well prior to the Liquidators opening their accounts portal;

63.5 the Liquidators' provisional acceptance of GNY's claim in its own name was, however, *after* the Liquidators had queried with GNY whether the accounts in question were GNY or personal accounts, and sought information and an explanation from GNY on why it considered the accounts to be its corporate accounts. GNY provided the Liquidators with

---

72 Ruscoe I, 31 July 2025, at [58]; [**201.0023**] at [**201.0040**].
73 Ruscoe I, 31 July 2025, at [57]; [**201.0023**] at [**201.0039**].
74 The point is made express in GNY's first engagement with the Liquidators: [redacted] 31 March 2025, [redacted]51; letter to Liquidators dated 10 July 2019, at [3]; [**201.0001**], [**302.0949**].
75 [redacted] 31 March 2025, [redacted]56 – Creditor Claim form, dated 9 July 2019; [**201.0001**], [**302.0949**] at [**302.0954**].
76 [redacted]31 March 2025, [redacted]04; [**201.0001**], [**303.1034**]. Note that the correspondence is clear throughout that Chapman Tripp's client (singular) is GNY.

the information and explanation necessary to demonstrate the accounts were, in fact, GNY accounts.[77] GNY explained (as it has had to do again in these submissions) that the Cryptopia accounts set up process could only be completed by natural persons, notwithstanding that Cryptopia knew that the accounts in question were GNY accounts.[78] The implication in the Liquidators' Submissions that GNY either failed to provide relevant documents, or relevant information, is therefore incorrect;[79]

63.6 the Liquidators provisionally admitted GNY's claim, in GNY's name, after GNY provided this explanation;[80]

63.7 relatedly, the Liquidators' new suggestion in their submissions that GNY failed to provide the information the Liquidators requested to establish whether the accounts in question were GNY or personal accounts[81] conflicts with the Liquidators' provisional acceptance at the time that GNY was the appropriate claimant in respect of the two accounts after reviewing the information GNY provided. No additional information on this issue has come to light since the Liquidators communicated their apparent acceptance that the accounts belonged to GNY – other than the Liquidators apparent reliance on their accounts portal process to demonstrate the accounts are personal accounts (addressed below); and

63.8 subsequent to all of this engagement with GNY, the Liquidators established their claims portal. Relevantly:

(a) the Liquidators required account holders to complete the portal to verify losses from trading accounts. GNY advised the Liquidators in correspondence that it should not be necessary for it to complete the portal

---

77 See correspondence in [redacted] 31 March 2025, [redacted]67 – 103, especially [redacted]-69, GNY letter to liquidators on 25 September 2019, at [63]–[66]; [**201.0001**], [**302.0957**] – [**303.1033**], [**302.0959**] at [**302.0971**].

78 See, for example, [redacted] 31 July 2025, [redacted] 9, GNY letter to liquidators on 25 September 2019, at [63]–[66]; [**201.0001**], [**302.0959**] at [**302.0971**].

79 Liquidators' Submissions, [8.27].

80 This occurred on 31 July 2020: [redacted] 31 July 2025, [redacted]104, Liquidators' letter to GNY on 31 July 2020, at [3]; [**201.0001**], [**303.10**].

81 Liquidators' Submissions, [8.27].

process in light of the Liquidators' provisional admission of GNY's claim in respect of its accounts[82] - but the Liquidators insisted that GNY complete their portal process;[83]

(b) but, as Mr Ruscoe explains in evidence, "the way we have established the accounts portal" is "on the basis that the account holders of Cryptopia… are the persons who have a contractual arrangement with Cryptopia by way of the terms and conditions".[84] Mr Ruscoe is also express that "our view is that Cryptopia's trust and contractual relationship is with [redacted] and [redacted] and not GNY".[85] In other words, [redacted] and [redacted] *could only successfully complete the portal requirements as the natural persons identified by the relevant account details*. If [redacted] had completed the portal on any other basis, GNY would reasonably have expected their account details to be rejected. Moreover, the (automated) portal process did not allow [redacted] to refer to or attach the material GNY had already submitted in connection with GNY's creditor claim; and

(c) [redacted] completed the portal accordingly – but safe in the knowledge that the Liquidators were already well aware that the two accounts were GNY accounts and had already "provisionally" admitted GNY's claim on the basis of GNY's prior explanation of the use of details of natural persons for the accounts. GNY engaged in the portal process only at the Liquidators' insistence, and on the understanding that the purpose of this engagement was to assist the Liquidators to verify the amount of LML remaining in the two accounts. Further, GNY's completion of the claims portal process was expressly on the basis that any correspondence between GNY's counsel and counsel for the Liquidators (being the

82 Alcartado I, 7 May 2026, PA1-22; [**401.0589**] at [**401.0613**].
83 Alcartado I, 7 May 2026, PA1-24 – 26; [**401.0589**] at [**401.0615**]- [**401.0617**].
84 Ruscoe I, 31 July 2025, at [57]; [**201.0023**] at [**201.0039**].
85 Ruscoe I, 31 July 2025, at [57]; [**201.0023**] at [**201.0039**].

correspondence relating to GNY's creditor claim against Cryptopia) should take precedence over any information provided through the claims portal.[86]

64 The Liquidators' implicit suggestion in their submissions that [redacted] may have committed a criminal offence by "misrepresentation of an unsecured creditor's identity"[87] in completing the claims portal is unwarranted as well as gratuitous.

65 The portal process is also irrelevant to the legal issues for the Court to determine concerning the accounts. The Liquidators' post-liquidation portal process has no bearing on whether the accounts are GNY accounts: this is a matter of contract law which is determined by the course of engagement between GNY and Cryptopia at the time that GNY began trading LML on the exchange through those accounts, not by events significantly after Cryptopia ceased trading altogether. All this episode shows is a certain vigorous level of resistance to GNY's claims.

Final comments on GNY accounts

66 In any event, even if the accounts were not GNY accounts on the basis outlined above, [redacted] are agents of GNY insofar as those accounts and associated contractual and other obligations are concerned.

67 It is well-settled that a corporate body such as GNY can only act by agents.[88] [redacted] had (and continue to have) implied actual authority from GNY with respect to all its engagement with Cryptopia, as [redacted] and [redacted]) (and it has never been suggested otherwise).[89] GNY was a disclosed principal.[90] Cryptopia was aware

---

86 Alcartado I, 7 May 2026, PA1-27 – 28 and PA1-31; [**401.0589**] at [**401.0619**] and [**401.0622**].

87 Liquidators' Submissions, [8.30].

88 *Aberdeen Railway Co v Blaikie Bros* (1854) 1 Macq. 461 at 471.

89 [redacted] roles are explained in his evidence, and referenced elsewhere in these submissions. See [redacted] confirmation of his roles: [redacted] 30 March 2025, at [5]; [**201.0012**] at [**201.0014**]. The Court of Appeal r [redacted] sed powers exercised pursuant to such roles are done so according to the actual implied authority arising from the individual's role in the corporate structure: *Giltrap City Ltd v Commerce Commission* [2004] 1 NZLR 608 (CA) at [40] and [42].

90 See Peter Watts and FMB Reynolds *Bowstead and Reynolds on Agency* (22nd ed, Sweet & Maxwell, London, 2021) at [1–035] where a disclosed principal is defined as "a principal... whose interest in the transaction as principal is known to the third party at the time of the transaction in question".

that that [redacted][91] that LML's listing on the Cryptopia platform was a GNY project, that the two accounts in question were the accounts into which LML was initially placed.

68 Given that Cryptopia's terms expressly allowed corporate traders – but such entities could only establish accounts using the details of natural persons – the accounts must have been established by [redacted] as GNY agents.

69 Given [redacted] roles at GNY, it is surprising that the Liquidators address submissions to the absence of "internal GNY documentation" about its ownership of the trading accounts in question.[92] It is unclear what internal authorisations the Liquidators would reasonably expect to see for [redacted] to take an operational step like opening a trading account on behalf of the company. In any event, GNY's internal documentation is irrelevant to the legal question of Cryptopia account ownership, which turns on GNY's engagement with, and arrangements with, Cryptopia.

70 In contrast to the Liquidators' approach, Cryptopia did not require any internal documentation from a company wanting to open an account and trade on the exchange. If a company wished to seek "Level 3" verification – permitting trading of up to $500,000 per 24 hours – Cryptopia would ask to see a bank statement connecting the account user to the company, or a link to a public register showing the account user as a company director – or, if the user was not a director, a handwritten statement confirming the account user was approved to trade on the company's behalf.[93] No such requirement was imposed for level 1 verification, or level 2 verification – being the verification stage which Cryptopia required GNY to meet in order to list and trade LML on the exchange.

---

91 See the Listing Form: Sibenik I, 1 August 2025, PJS1-8; [**201.0090**], [**302.0719**].
92 Liquidators' Submissions, [8.34]
93 Cryptopia Customer Service Manual, Brocket I, 27 November 2019, TJSB1-45; [**401.0194**] at [**401.0245**].

SECTION 5: CRYPTOPIA'S CYBERSECURITY FAILURES

71 Cryptopia's defective cybersecurity posture underpins GNY's legal claims against Cryptopia. Before turning to each head of claim, it is worth giving an overview of the Cryptopia failings on which those claims are based, and explaining the factual basis on which those failings were legally causative of the losses arising from the Hack.

Expert evidence

72 The expert evidence is clear that Cryptopia's approach to cybersecurity through 2018-2019 fell significantly short of what could reasonably be expected of a cryptocurrency exchange such as Cryptopia.

73 GNY's cybersecurity expert, Mr Dicks, undertakes a thorough review of Cryptopia's cyber-settings in 2018-2019 in his evidence.

74 Mr Dicks' conclusions are damning.

75 Mr Dicks concludes that Cryptopia's security measures fell "well short" of an appropriate standard for a cryptocurrency exchange operating in 2018-2019, and the platform was "very vulnerable" to attacks.[94]

76 Cryptopia's systems were sufficiently immature that they "could not prevent even a low to modestly skilled attacker from gaining full access to Cryptopia's wallet environment undetected".[95]

77 Mr Dicks identifies no fewer than 55 material vulnerabilities in Cryptopia's cybersecurity settings, despite Cryptopia being at high-risk of an attack. He describes an "overall picture… of a highly vulnerable network, which had not adopted routine cybersecurity protections available that were in widespread use in 2018".[96]

78 Among the most serious deficiencies in Cryptopia's cybersecurity settings was its failure to adopt network segregation. Mr Dicks explains:[97]

---

94 Dicks I, 18 December 2025, at [12.1]; [**201.0154**] at [**201.0157**].
95 Dicks I, 18 December 2025, at [12.4]; [**201.0154**] at [**201.0158**].
96 Dicks I, 18 December 2025, at [52]; [**201.0154**] at [**201.0172**].
97 Dicks I, 18 December 2025, at [19.3]; [**201.0154**] at [**201.0161**].

> Network segregation either prevents attackers moving laterally through the network, or at the very least slows those attackers down considerably. Network segregation is critical to any effective cybersecurity model. Network segregation was a well-established and routine security measure by 2018.

79 The Liquidators' cybersecurity expert, Mr Watson, agrees with Mr Dicks that:

> A consistent finding across them all [Cryptopia's cybersecurity reports], was that "insufficient network segregation" existed. The ramification of this finding is that should an attacker gain unauthorised access it would potentially be possible to move throughout the network (lateral movement) gaining additional access and privileges.

80 In his evidence, Mr Dicks analyses the detailed feedback which Cryptopia received through the course of 2017 and 2018 from Pulse Security (**Pulse**), an organisation Cryptopia engaged to diagnose (but not fix) existing vulnerabilities in its cybersecurity posture.

81 The Pulse reports, and Mr Dicks' analysis of those reports, make for sobering reading. In summary:

81.1 Cryptopia initially engaged Pulse in November 2017;

81.2 Pulse's 14 November 2017 report providing an overview of Cryptopia's cybersecurity arrangements raised serious concerns about the inadequacy of those arrangements. It identified numerous material weaknesses in Cryptopia's basic security settings.[98] As Mr Dicks explains, "Pulse was able to breach Cryptopia's security easily and without sophisticated tools – twice";[99]

81.3 subsequently, Pulse was able to penetrate and enter Cryptopia's wallet environment without detection again: it did so in tests it undertook and described in reports it prepared dated 27 November 2017, and 28 February 2018 again easily. Both test reports identified further material and unacceptable weaknesses in Cryptopia's security settings;[100]

---

98 Ruscoe I, 31 July 2025, DIR1-111 – 119; [**201.0023**] at [**301.0137**] to [**301.0145**].

99 Dicks I, 18 December 2025, at [38]; [**201.0154**] at [**201.0166**].

100 See Ruscoe I, 31 July 2025, DIR1-120 (Red Team Penetration Test Report) and DIR1-184 (Red Team Engagement Report); [**201.0023**] at [**301.0147**] and [**301.0284**].

81.4 Pulse produced at least eight other reports for Cryptopia between December 2017 and August 2018 on various aspects of Cryptopia's cybersecurity settings, all of which were diagnostic not remedial. All identified serious – and in some cases astonishingly basic – cybersecurity weaknesses;[101]

81.5 among the most appalling examples of lax cybersecurity practices at Cryptopia, Pulse identified that Cryptopia's external firewall was reliant on a default "admin" password obtainable by any person simply by searching the internet for the default settings provided with the firewall product when purchased off the shelf.[102] In another instance, Pulse identified that Cryptopia staff adopted obviously poor password practices – such as using variants on the word "password", or use of default login details.[103] These are examples only: nearly every Pulse report identifies rudimentary security failings;

81.6 in addition, as Mr Dicks explains in his evidence, nearly all of the Pulse reports pointed out that Cryptopia had failed to implement appropriate network segregation, a basic cybersecurity measure, and a vulnerability which the attackers ultimately exploited in the Hack.[104]

82 Mr Dicks' conclusions about the nature of the 55 serious cybersecurity deficiencies he identified at Cryptopia are equally sobering. Mr Dicks' expert opinion is that Cryptopia's cybersecurity failings were systemic, inappropriate for a business of Cryptopia's nature – and were notified to Cryptopia repeatedly over the space of 18 months prior to the Hack:[105]

> … [a] recurring theme in the material I have reviewed is that several serious weaknesses were identified more than once, in particular serious concerns regarding a lack of network segmentation, red-team access to wallet systems, credential handling and monitoring.

---

101 Mr Dicks describes each of these eight reports in his evidence: Dicks I, 18 December 2025, at [40]; [**201.0154**] at [**201.0166**].
102 Dicks I, 18 December 2025, at [40.4]; [**201.0154**] at [**201.0168**]; and see the Pulse report at Ruscoe I, 31 July 2025, DIR1-214; [**201.0023**] at [**301.0314**].
103 Dicks I, 18 December 2025, at [40.5]; [**201.0154**] at [**201.0168**]; and see the Pulse report at Ruscoe I, 31 July 2025, at DIR1-222; [**201.0023**] at [**301.0325**].
104 Dicks I, 18 December 2025, at [53.2] and [59]; [**201.0154**] at [**201.0172**] and [**201.0174**].
105 Dicks I, 18 December 2025, at [55]; [**201.0154**] at [**201.0173**].

83 Mr Dicks' assessment is more definitive than the assessment of Mr Watson. Overall, however, the conclusions of the two experts overall on this topic are very similar.

84 In his primary evidence, Mr Watson:

84.1 was instructed to give a view on whether Cryptopia "[h]ad taken reasonable steps to prevent a compromise of their network and systems".[106] Interestingly, Mr Watson does not directly answer that question;

84.2 Mr Watson's evidence certainly does not give any basis to conclude that Cryptopia had taken "reasonable steps" on cybersecurity. His evidence on this issue is to the effect that:

(a) there is no evidence Cryptopia developed or implemented a formal cyber-security framework;[107]

(b) Cryptopia "did not have anyone solely tasked with the oversight of cyber-security internally at Cryptopia";[108]

(c) "No evidence has been found that Cryptopia had the capacity to monitor, detect, investigate or respond to a cyber attach by means of a managed Security Operations Centre (SOC) or that it had the capability to collect and analyse security logs or events (Security Information and Event Management – SIEM). The SOC, and SIEM capabilities… would be critical in forming a comprehensive cyber security capability within a high-risk organisation".[109] Both Mr Watson and Mr Dicks agreed that Cryptopia was a high-risk organisation;

(d) it would be "incorrect to suggest that Cryptopia did not address cyber security".[110] But Mr Watson does not express a view on whether the way in which Cryptopia

106 Watson I, 31 July 2025, at [3(a)]; [**201.0072**] at [**201.0073**].
107 Watson I, 31 July 2025, at [13]; [**201.0072**] at [**201.0076**].
108 Watson I, 31 July 2025, at [13]; [**201.0072**] at [**201.0076**].
109 Watson I, 31 July 2025, at [13]; [**201.0072**] at [**201.0076**].
110 Watson I, 31 July 2025, at [14]; [**201.0072**] at [**201.0076**].

"addressed" cyber security was reasonable, or appropriate, or not. He notes in this regard:

(i) Cryptopia prepared a document (in approximately May 2018 and described as an Infrastructure Plan on its face) addressing "growth and improvement in The Company Infrastructure", which contained recommendations relevant to enhancement of security.[111] But Mr Watson recognises that it is unclear whether the author gave consideration to (failed) Pulse penetration testing results, and "no evidence has been identified… that would provide any insight as to the proposed response by management [to the paper]… or whether there was any planned implementation of the recommendations made".[112] Put another way, it is not clear to Mr Watson whether any of the recommendations made were actually implement. And, as Mr Watson implies and Mr Dicks expressly confirms, the paper did not actually address the serious vulnerabilities already identified by Pulse;[113]

(ii) Pulse testing and diagnostic assessments "identified vulnerabilities of varying severity" but "no evidence has been identified by the liquidators that would provide insight as to what the "planned changes" were, nor the timeframe for implementation of the recommendations".[114] Again, put another way, it is not clear to Mr Watson what changes were actually implemented to address Pulse's recommendations.

---

111 Watson I, 31 July 2025, at [15]; [**201.0072**] at [**201.0076**].
112 Watson I, 31 July 2025, at [20]–[21]; [**201.0072**] at [**201.0078**].
113 See Dicks I, 18 December 2025, at [64]–[66]; [**201.0154**] at [**201.0175**] to [**201.0176**].
114 Watson I, 31 July 2025, at [22]–[28], quoting [28]; [**201.0072**] at [**201.0078**].

85 Overall, Mr Watson's evidence identifies a range of serious vulnerabilities in Cryptopia's cybersecurity posture, notes that Cryptopia did "address" cyber security (without giving a view on sufficiency of how the topic was addressed) and concludes that there is not enough evidence for Mr Watson to know whether Cryptopia implemented Pulse's recommendations to address its vulnerabilities, or not.

86 Mr Watson is clearer on the reasonableness, or otherwise, of Cryptopia's cybersecurity posture in his reply evidence, which confirms "I do not think Mr Dicks says anything fundamentally different to the opinion I provided in my first affidavit".[115] Mr Watson does not take issue with, let alone disagree with, any of Mr Dicks' analysis of the 55 vulnerabilities with Cryptopia's cybersecurity posture which he describes in his evidence.

87 Mr Watson's reply is revealing, however, of what is ultimately the primary difference between his evidence and Mr Dicks' evidence. That primary difference is not a matter of a different expert opinion, but a difference in reasoning approach. Mr Watson says in his reply:

> As of 2019, Cryptopia was of sufficient scale (at least from an asset and trading perspective) that I would have expected a plan to have been devised, if not implemented, subsequent to Pulse's testing. *Although we have not been presented with such a document, I cannot definitively state whether or not such a document existed.*
>
> (emphasis added)

88 Mr Watson treats the absence of a document as uncertainty as to whether the document existed, or not. His evidence is, in this respect, more conservative than Mr Dicks (noting again that this difference is not really a matter of expertise: on those matters, the experts largely agree).

89 While it is technically the case that the absence of a thing does not prove that thing never existed, there is a more commonsense approach to the absence of any Cryptopia plan to address its significant cybersecurity vulnerabilities than the approach Mr Watson adopts.

---

115 Watson II, 28 January 2026 (reply), at [3]; [**201.0252**] at [**201.0253**].

90 Cryptopia's records do not contain a cybersecurity plan to address the serious vulnerabilities identified in the Pulse testing. Nor is there mention of any such plan in Cryptopia's emails. There is no receipt or order of work for an external provider to create such a plan in Cryptopia's records. And there is no mention of any such plan in any of the comments made by Cryptopia's directors and officers when interviewed by the liquidators after Cryptopia's collapse. It is highly probable that this absence of records is because Cryptopia *did not actually devise a plan* to address the serious vulnerabilities identified by Pulse – let alone implement one.

Liquidators' position

91 Notwithstanding that the parties have both engaged experts to comment on the reasonableness, or appropriateness, of Cryptopia's cybersecurity posture, and notwithstanding that the parties' experts are substantially in agreement on this topic, the Liquidators have optimistically submitted that "Cryptopia's security measures may have been reasonable".[116] Towards the end of their submissions, the point is put in even stronger terms: "it is not clear what more the reasonable person could have or would have done in the circumstances".[117]

92 In addition to the expert analysis:

92.1 the Liquidators rely on purported cybersecurity measures which neither Mr Watson nor Mr Dicks considered relevant enough to address in their evidence on this topic. In some of these cases, the measures relied on by the Liquidators pre-date Cryptopia failing the Pulse penetration testing (suggesting the measure is irrelevant to the vulnerabilities identified in that testing),[118] and in some cases the measures relied on by the Liquidators are not cybersecurity measures at all;[119]

---

116 Liquidators' Submissions, [8.131].
117 Liquidators' Submissions, [9.14].
118 For example, account creation standards Liquidators' Submissions, [8.110]; or DDOS protection software Liquidators' Submissions, [8.114].
119 For example, investment in infrastructure building is different from cybersecurity protections for that infrastructure. See references to Cryptopia's engagement of Red Rabbit Tech and Inde Technology, Liquidators' Submissions at [8.1114]. Mr Dicks confirms in his evidence that Cryptopia's engagement of Inde Technology likely related to infrastructure, not cyber-security: Dicks I, 18 December 2025, at [75]; [**201.0154**] at [**201.0179**].

92.2 the Liquidators provide narrative explanations for Cryptopia's conduct which are not supported by Cryptopia records or any other source. For example, the Liquidators' claim that Cryptopia engaged Pulse because of its "growing user base and likely because there were no recognised security standards"[120] is speculative, as are a number of comments about what "practices would be expected of any cryptocurrency exchange".[121] Several of the narrative descriptions which the Liquidators offer for Cryptopia on cybersecurity matters are in tension with characteristics they bestow on Cryptopia when addressing other topics: for example, in connection with cybersecurity, the Liquidators describe Cryptopia as a relatively young company experiencing teething issues,[122] purportedly with no cybersecurity expertise.[123] But in connection with Representations, Cryptopia is described as "the fourth largest cryptocurrency exchange in the world" with "one of the largest number of cryptocurrencies listed on any exchange at the time" and therefore the Liquidators say it is true to describe Cryptopia as a "leading and trusted exchange";[124]

92.3 similarly, the Liquidators describe Cryptopia's "consideration" of various different providers of cybersecurity services through the course of 2018[125] and conclude that "there did not appear to have been viable options available to Cryptopia for a full-scale security review".[126] That conclusion is not supported by any expert assessment of those options, nor any comments from Cryptopia's directors or managers. The reality is that Cryptopia did not pursue any of the options it considered to improve its cybersecurity. The reason why does not need to be speculated on. The actual explanation for Cryptopia's decision-making is identifiable from Cryptopia's documentary records. These records make clear that Cryptopia chose to deprioritise addressing its known cybersecurity vulnerability in favour of spending on other

120 Liquidators' Submissions, [8.112].
121 Liquidators' Submissions, [8.1119].
122 Liquidators' Submissions, [8.128].
123 Liquidators' Submissions, [8.130].
124 Liquidators' Submissions, [8.110(b)].
125 Liquidators' Submissions, [8.124]–[8.125].
126 Liquidators' Submissions, [8.125].

priorities, despite objections from its senior technical staff to this approach.[127]

92.4 the material referred to by the Liquidators to demonstrate Cryptopia's purported cybersecurity efforts is also highly selective. For example, the Liquidators do not acknowledge the comments in a number of Cryptopia records which point to Cryptopia ignoring known cybersecurity vulnerabilities – and which confirm that, as at May 2018, Cryptopia's management and directors positively *refused* to attest to the current state adequacy of its cybersecurity measures.[128] Put another way – even Cryptopia understood its cybersecurity posture was not reasonable before the Hack occurred.

93 In any event, as the Liquidators properly accept, a failure to adopt "consistent cold wallet practices" may be a failure to take reasonable steps to protect cryptocurrency from the Hack.[129]

94 The Liquidators appear to be unsure as to whether Cryptopia did fail to adopt such practices for ETC currencies, notwithstanding that all available evidence suggests that Cryptopia's hot and cold wallet practices were inconsistent generally, that no cold wallet system was ever implemented for ETC,[130] and all of Cryptopia's ETH holdings were actually stored in a hot wallet at the time of the Hack and therefore highly vulnerable to that Hack – including LML.[131] There is no evidence to suggest that Cryptopia's storage approach to ETC coins (the majority of which were stolen in the Hack) was planned or appropriate, or involved any cold wallets at all.

95 Finally, the Liquidators are critical of Mr Dicks' evidence, notwithstanding that Mr Watson largely agrees with Mr Dicks.

96 In part, the Liquidators seek to downplay Mr Dicks' analysis and conclusions by claiming that there was no clearly applicable, objective standard against which to measure whether Cryptopia's cybersecurity posture was reasonable, or appropriate, or not.[132]

---

127 See [**143**] – [**160**] below.

128 See [**143**] – [**160**] below.

129 Liquidators' Submissions, [8.138].

130 See Liquidators' Submissions, [8.132]–[8.136].

131 See Liquidators' Submissions, [8.132]–[8.136].

132 Liquidators' Submissions, [8.115]–[8.118].

That is a red herring. It is better to call a spade a spade. The absence of a singular standard does not mean it is impossible to measure whether an organisation's cybersecurity settings are appropriate or reasonable. As Mr Dicks explains in his evidence (with no disagreement from Mr Watson):[133]

> [23] It is difficult to implement fixed legal rules for cyber-security for a number of reasons: technical solutions are not always one-size-fits-all, business needs and risk profiles differ, and technology (and cyber-security risks) are dynamic and forward-looking to name a few.
>
> [24] However, this does not mean there are not benchmarks to address the adequacy of organisational settings against, and documents like NZISM and the Australian guidance provide publicly available reference points for what good practice looks like, particularly for organisations with high cyber-security needs like Cryptopia.
>
> [25] By 2018, there were also several well-known and well-regarded compliance standards that were in use globally in the cyber-security industry, and widely used benchmarks for private sector organisations..
>
> …
>
> [26] Not all organisations sought out formal certification. Not every organisation would need to comply with every element of each available framework depending on a combination of factors such as organisational size, resources and cyber-security risks / needs. Again, however, these internationally recognised standards provide valuable best practice benchmarks for organisational security.

97 Relatedly, the Liquidators criticise Mr Dicks on bases that are simply inaccurate descriptions of what he does in his evidence. For example, dismissing his evidence as affected by "hindsight"[134] despite Mr Dicks' care to apply 2018 standards to his assessment.[135] Or incorrectly suggesting that Mr Dicks did not consider "the context of cryptocurrency exchanges at the time (or Cryptopia's specific circumstances)",[136] when Mr Dicks plainly does exactly that,[137] including when expressly concluding that Cryptopia's cybersecurity posture falls well short of the standard he would expect of a cryptocurrency exchange in 2018.[138] And wrongly implying that Mr Dicks applied a "best-practice" rather than "reasonable" standard to his assessment.[139]

---

133 Dicks I, 18 December 2025; [**201.0154**].
134 Liquidators' Submissions, [8.130]
135 See Dicks I, 18 December 2026, section (3); [**201.0154**] at [**201.0159**].
136 Liquidators' Submissions, [8.129].
137 See, for example, only, Mr Dicks' assessment of Cryptopia's specific risk profile (section (4)), specific vulnerabilities (also section (4)), specific warnings (also section (4)); [**201.0154**] at [**201.0164**].
138 Dicks I, 18 December 2025, section (5); [**201.0154**] at [**201.0171**].
139 Liquidators' Submissions, [8.129].

98 On the last point, Mr Dicks' instructions were to assess whether Cryptopia's cybersecurity measures were appropriate for an organisation operating a cryptocurrency exchange in 2018. Mr Dicks treated 'appropriate' and 'reasonable' interchangeably as can be seen, for example, in this conclusion:[140]

> [49] In my view, Pulse Security's testing revealed that Cryptopia's cyber-security posture fell well short of the standard I would expect of a cryptocurrency exchange in 2018 – particularly one known to be at risk of a state-sponsored attack.
>
> [50] This is an evaluative assessment, rather than applying clear "pass / fail" criteria. *However, in my view, Cryptopia's cyber-security posture in 2018-2019 was so weak that it is clearly the case that its cyber-security arrangements were unreasonable and inappropriate for a business of its nature and cyber risk profile.*
>
> (emphasis added)

99 If the purpose of these criticisms by the Liquidators is to suggest that there is some room for ambiguity about whether Cryptopia's cybersecurity posture was reasonable, that proposition is unsustainable in light of Mr Dicks' analysis, and Mr Watson's acceptance of that analysis. That expert analysis, in turn, accords with commonsense. There is no room for doubt about whether Cryptopia's cybersecurity measures may have been reasonable or appropriate – let alone best practice. Again, the fact that the Liquidators have sought so hard to shade black into grey is itself revealing.

The Hack was preventable

100 The evidence also suggests that if Cryptopia had adopted adequate cybersecurity measures, the Hack could likely have been prevented, or detected and halted quickly once it was underway.

101 Mr Watson's evidence is that it is "impossible" to "definitively" conclude that the Hack could have been identified and prevented.[141] This is because "no security can be thought of as 100% effective".[142]

102 While Mr Watson appears to accept that most APT attacks are preventable, he is also of the view that some attacks of this nature

---

140 Dicks I, 18 December 2025; [**201.0154**] at [**201.0171**].
141 Watson I, 31 July 2025, at [54]; [**201.0072**] at [**201.0084**].
142 Watson I, 31 July 2025, at [54]; [**201.0072**] at [**201.0084**].

would be successful.[143] In his view, he does not have "enough evidence to definitively conclude whether the Hack was sophisticated or preventable".[144]

103 Of course, little in life can be regarded as 100% guaranteed. That trope is, here, irrelevant. Mr Watson's logic is incompatible with a balance of probabilities assessment: GNY need not "definitively" demonstrate that the only possible outcome if Cryptopia had adopted basic security measures is that the Hack would have been prevented. It need show only that it is more likely than not that the Hack would have been prevented or stopped before material harm resulted if Cryptopia had implemented adequate security measures before the Hack occurred.

104 All of the available evidence supports the conclusion that the Hack was likely to have been preventable, or stopped before harm occurred, if Cryptopia had adopted the basic security measures which Mr Dicks describes in his evidence.

105 It is relevant that:

105.1 the "impossibility" conclusion Mr Watson reaches in his evidence reflects his concern about the limited available information about how the Hack unfolded. This information limitation is, in large part, because of Cryptopia's own failures or lack of action. Specifically, neither Cryptopia nor the liquidators undertook a forensic analysis of the Hack, and Cryptopia did not have any sufficient monitoring system to observe and record attack pathways as it occurred.[145] Lack of monitoring and detection capability is one of Mr Dicks' 55 identified cybersecurity vulnerabilities. Cryptopia can hardly rely on its own technological failures to defend a claim that those failures existed;[146]

---

143 Watson II, 28 January 2026 (reply), at [16]–[17]; [**201.0252**] at [**201.0255**].
144 Watson II, 28 January 2026 (reply), at [16]; [**201.0252**] at [**201.0255**].
145 Dicks I, 18 December 2025, at [76]–[78] and [96]–[97]; [**201.0154**] at [**201.0180**] and [**201.0185**]. See also Mr Dicks' description of Cryptopia's lack of SOC and SIEM monitoring systems: issues [98.5] & Schedule 2 Issues 3 & 4**.** Mr Watson notes the same deficiencies in his first affidavit dated 31 July 2025 at [13]; [**201.0072**] at [**201.0076**].
146 Watson I, 31 July 2025, at [54]; [**201.0072**] at [**201.0084**].

105.2 Mr Watson does not, in any event, appear in his main report to have even considered whether the information that is available about the Hack informs whether it is likely that the Hack could have been prevented, or not. This is not a question Mr Watson addresses;

105.3 as Mr Dicks explains, the information we do know about the Hack suggests that the attacker's methodology was not, in fact, overly sophisticated. For example, the Hack commenced using a very common phishing attack delivery mechanism: a malicious email link.[147] Mr Watson appears to accept in his reply evidence that the available information (supplied by the New Zealand Police) "does not detail a sophisticated attack";[148]

105.4 equally importantly, we know that the Hack methodology exploited weaknesses which Cryptopia had been repeatedly warned about in multiple reports prepared by its cybersecurity advisors, Pulse;

105.5 specifically, the hackers utilised Cryptopia's lack of network segregation to move easily and without resistance through parts of the Cryptopia network, and to readily access its wallet environment.[149] We also know that Cryptopia's failure to adopt immutable logs (a vulnerability Cryptopia was also warned about by Pulse) enabled the attackers to delete traces of the attack vector easily;[150]

105.6 Mr Dicks identifies a range of other contextual factors which tend to suggest that Cryptopia would have been far less susceptible to the Hack occurring or resulting in cryptocurrency theft if it had adopted adequate security measures. These factors include the lack of any obvious need

---

147 Dicks I, 18 December 2025, at [82]; [**201.0154**] at [**201.0180**].
148 Watson II, 28 January 2026 (reply), at [13]; [**201.0252**] at [**201.0255**].
149 Dicks I, 18 December 2025, at [82] and [98]; [**201.0154**] at [**201.0180**] and [**201.0186**].
150 Dicks I, 18 December 2025, at [82] and [98]; [**201.0154**] at [**201.0180**] and [**201.0186**]. The Liquidators suggest in their submissions that Mr Dicks is speculating about the ease with which the hackers will have been able to delete Cryptopia's logs (at [8.161]). This is incorrect. As he states in his evidence, this was a weakness in Cryptopia's system identified by Pulse in its reports, and it is analysed in detail by Mr Dicks. See [55.3] of his evidence, and issues 3, 7, 9, 41, 50 and 55 of his detailed Issues Schedule.

for hackers to adopt a highly sophisticated attack method given Cryptopia's lack of cybersecurity protections, and Cryptopia's defencelessness once the Hack commenced – this due to the total absence of monitoring and defensive mechanisms to identify and stop an attack occurring in real time across its network; and

105.7 in addition, Mr Dicks points out that most APT attacks across the world are, in fact, prevented by organisations which adopt the basic security measures Cryptopia failed to adopt (like network segregation) – and the effectiveness of these basic security measures against APT attacks is what enables the vast majority of online commerce.[151]

106 Having reviewed Mr Dicks' comments in his evidence, Mr Watson appears to accept a material part of Mr Dicks' expert analysis in his reply:[152]

> 16. …I think it is too simplistic to say just because an organisation adopts "adequate risk management and detection capabilities" that most APT attacks are preventable. It is reasonable to assert that with adequate risk management and detection capabilities an organisation is in an immeasurably better position to identify and prevent such an attack. That said, by stating that "most" attacks are definitively preventable, that does of course allow that "some" would be successful. I return to the fact we simply do not have enough evidence to definitively conclude whether or not the Hack was sophisticated or preventable.
>
> 17. At paragraphs [89] and [98], Mr Dicks opines that if Cryptopia had implemented appropriate detection, monitoring and response capabilities, then it would have been able to isolate the attacker's movements early on. I agree that Cryptopia would have potentially identified the Hack earlier and would have been in a better position to potentially prevent it.

107 Taking Mr Watson at face value, he appears to accept that if Cryptopia had adopted adequate risk management and detection, it would have been in an "immeasurably better position to identify and prevent such an attack", and if it had adopted appropriate response capabilities, it could potentially have isolated the attacker early on after the Hack commenced. His comments here support the conclusion that, on balance of probabilities, the Hack was preventable had adequate cybersecurity measures been in place.

---

151 Dicks I, 18 December 2025, at [98]; [**201.0154**] at [**201.0186**].
152 Watson II, 28 January 2026 (reply); [**201.0252**] at [**201.0255**].

108 Again, however, the Liquidators take a position in their submissions that is difficult to reconcile with the totality of the expert opinion evidence.

109 For example, they suggest that, because the Hack is suspected to have been undertaken by the DPRK, this suggests that "… the Hack was sophisticated, advanced and exceptional… it would be exceedingly difficult, if not impossible, to repel, regardless of the security measures in place."[153] Mr Dicks is certainly not of that view. Nor does Mr Watson go to this extreme. Mr Watson simply says of the suspected hackers: "you could reasonably describe them as sophisticated".[154]

110 To support their submission that the Hack was exceptional and likely impossible to repel, the Liquidators point to a range of publicly reported successful APT hacks from around the world before concluding "[t]hese example demonstrate that even prominent and well-resourced exchanges have been unable to prevent determined cyber-exchanges".[155]

111 This is flawed reasoning, drawing invalid conclusions between anecdotal evidence and base-rate statistical attributes.[156] Only successful attacks make headlines or result in litigation. The fact that we know these attacks succeeded does not tell us anything about whether all attacks succeed, or only some, or their nature, and nothing about whether the hack methodology used in the Cryptopia Hack was unstoppable, or not. Nor do we have any evidence about the cybersecurity measures in place at the hacked organisations. So reference to other attacks in other unknowable contexts is ultimately uninformative. Again, the question arises as to why the Liquidators are going to such lengths to characterise the Hack in this way. A better course than advocacy would surely have

---

153 Liquidators' Submissions, [8.157].
154 Watson II, 28 January 2026, at [14]; [**201.0252**] at [**201.0255**].
155 Liquidators' Submissions, [8.116].
156 In *Rationality*, Steven Pinker provides a comparable example of this logical fallacy in his discussion of the availability heuristic: that anecdotes and experiences become the basis for an individual's approximation of the probability of a given event ((Penguin Press, United Kingdom, 2022) at 119). This can be further affected by media: "The press is an availability machine. It serves up anecdotes which feed our discussion our impression of what's common in a way that is guaranteed to mislead" (at 125). Pinker goes on to say that media coverage drives people's sense of frequency and risk. One example of this is that people think they are likelier to be killed by a tornado than by asthma, despite asthma being eighty times deadlier due to the greater news coverage of one over the other (at 120).

been to investigate and advise conclusions based on a detailed forensic report. But that is exactly what we do not have.

112 The Liquidators also suggest, in what appears to be an entirely hypothetical sequence of events beginning from October 2018 based on a range of unexplained assumptions, that Cryptopia could not have remedied its identified cybersecurity flaws before the Hack occurred in January 2019.[157]

113 October 2018 is of no significance other than being the date of the last available internal Cryptopia record (its "virtual CISO" [Chief Information Security Officer] report) confirming its cybersecurity status was far below what is required for a cryptocurrency exchange.[158] Cryptopia was aware of the urgent need to take action well before then. More relevantly, see Pulse's initial "Consulting Summary", prepared when Pulse was first engaged to make recommendations regarding Cryptopia's cybersecurity settings. This document – from November 2017 – highlighted critical vulnerabilities requiring high priority to fix.[159] Or the first time Cryptopia failed rudimentary penetration testing – also in November 2017.[160] Or the second time Cryptopia failed basic penetration testing – in February 2018.[161] Or when its Operations Manager warned its senior managers and directors that they should not be able to sleep at night because of the critically vulnerable state of the platform's cybersecurity – in February 2018.[162] Or when the New Zealand government advised Cryptopia it was an identified cyberattack target, and at imminent risk of an attack occurring – in March 2018.[163]

114 The Liquidators' own expert evidence suggests that if Cryptopia had taken action at any one of those points in time, the action required

---

157 See Liquidators' Submissions, [8.124]–[8.126].
158 Ruscoe I, 31 July 2025, at [82]; [**201.0023**] at [**201.0046**].
159 Ruscoe I, 31 July 2025, DIR1-111 – 119; [**201.0023**] at [**301.0137**] to [**301.0145**].
160 Ruscoe I, 31 July 2025, DIR1-112; [**201.0023**] at [**301.0138**].
161 Ruscoe I, 31 July 2025, DIR1-184; [**201.0023**] at [**301.0284**].
162 Ruscoe II, 4 November 2025, DIR2-296 – 298; [**201.0117**] at [**301.0276**] to [**301.0278**].
163 Ruscoe I, 31 July 2025, at [73]; [**201.0023**] at [**201.0043**].

was both affordable for Cryptopia, and would have been completed well before the Hack occurred.[164]

115 Primarily, however, the Liquidators adopt Mr Watson's reasoning approach: (A) Because *some* APT hacks are unpreventable, (B) exchanges cannot "entirely eliminate the risk of a successful hack",[165] therefore (C) it cannot be ruled out that Cryptopia Hack was unpreventable without knowing more information about the Hack methodology.

116 As noted earlier, this approach to informational uncertainty is inconsistent with a balance of probabilities assessment. It also fails to account for the damning problem that Cryptopia's lax approach to security made it ripe to be plucked by an ordinary hack. Given Cryptopia's vulnerability, it is mere speculation that the actual hack was of a kind that Cryptopia could not have repelled even had it put in place reasonable cybersecurity measures – which it had not. Cryptopia was a sitting duck. When a sitting duck gets stolen, the onus is on those who say it would have been taken anyway to so establish. The Liquidators do not attempt to shoulder this burden. The balance of probabilities conclusion is that, whilst it is possible (because little in life is 100% guaranteed) that the Hack may still have occurred had Cryptopia put in place adequate security measures, that conclusion cannot be said to be likely. The Liquidators' attempt to reason otherwise would have visit the consequences of the relative lack of available information about the Hack methodology entirely on GNY and other Hack victims – despite that the information deficit being Cryptopia's own fault.

117 The proper approach is as described above: the available evidence, and the expert analysis of that evidence, supports the conclusion that if Cryptopia had addressed its material cybersecurity weaknesses, the Hack was likely to have been preventable, or stopped before damage occurred.

---

164 Watson II, 28 January 2026, at [6]–[8]; [**201.0252**] at [**201.0253**] to [**201.0254**].
165 Liquidators' Submissions, [8.166].

SECTION 6: CRYPTOPIA IS LIABLE FOR HACK LOSSES

Cryptopia's breach of fiduciary duty

118 Cryptopia was, ultimately, highly and unacceptably vulnerable to the Hack. Had it adopted appropriate, reasonable cybersecurity measures, it would likely have prevented or stopped the Hack.[166]

119 What legal consequences flow from this for Hack victims like GNY?

120 All GNY's LML on the exchange was stolen in the Hack.[167] The effect of the Hack on the market capitalisation of LML was catastrophic.[168]

Cryptopia's fiduciary obligations

121 One consequence is that Cryptopia breached its fiduciary duties to GNY. Cryptopia was a trustee of GNY's LML tokens held in Cryptopia trading accounts.[169] As trustee, Cryptopia is responsible for all GNY's losses arising from the Hack. Those losses occurred because Cryptopia's dereliction of duty was so profound as to amount to a breach of its duty to act in good faith with respect to GNY. GNY is accordingly entitled to equitable compensation from Cryptopia reflecting the full extent of its losses arising from the Hack.

122 Cryptopia is, naturally, accountable for the way in which it carried out duties imposed on it as trustee by the law.[170] At present, those duties include the default duties in ss 23-27 of the Trusts Act 2019 (**TA**), and the mandatory duties in ss 29-38.[171] These statutory duties are not new expressions of trustee obligations: the TA codifies trustee duties generally in effect prior to the enactment of the TA. The extent of what is required to discharge those duties vary in accordance with the nature of the trust, its circumstances, and the extent (and discretion) of powers afforded to the trustee by the trust terms.

---

166 As noted above from [**100**]–[**117**].

167 See [redacted] 31 March 2025, at [15]; [**201.0001**] at [**201.0004**] .

168 See [redacted] 31 March 2025, at [19]–[21]; [**201.0001**] at [**201.0004**] to [**201.0005**]: also see the evidence of Mr O'Shea valuing GNY's lost LML market capitalisation; [**201.0246**] at [**304.1476**].

169 See *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728, [2020] 2 NZLR 809; [**401.0365**].

170 Trusts Act 2019, s 13(b).

171 While the Trusts Act 2019 did not apply at the time of the Hack, it does now, and it is a codification of existing duties rather than a revision of law. Therefore, it is convenient to refer to it to summarise applicable principles.

123 While the Liquidators have suggested that Cryptopia may not have owed a range of ordinary trustee duties in holding trust property,[172] their rationale for this suggestion is somewhat unclear.

124 The Liquidators say that a range of duties found in the TA duties were not codified in the Trustee Act 1956 (correct but irrelevant: the 1956 Act did not codify trustee duties), nor included in the Terms and Conditions (not strictly correct: the Terms and Conditions explicitly recognised a duty of reasonable care. See clause 8(a), in which Cryptopia promises to "use *reasonable care* in operating our Platform"[173]). While the Liquidators suggest elsewhere in their submissions that this obligation in the Terms and Conditions was limited to maintenance disruptions,[174] this is also incorrect: the commitment to limit disruptions concerns all "Platform Change" and "Business Disruptions" without qualification, and maintenance disruptions is referred to in the clause as one type of such disruption only (… it may *also* be inaccessible from time to time while undergoing maintenance…).

125 In any event, a trustee's overriding to preserve trust property applies equally to a bare trustee, and in exercising that duty, trustees have a general duty of care.[175] These obligations are articulated in case law, irrespective of whether they are made express in the terms of the trust in question. Where, as here, the Court has already found that Cryptopia's "principal duty" was to "hold the pool of currency… on behalf of those accountholders",[176] it is plain that, unless excluded, Cryptopia was required to exercise reasonable care in holding account holder's cryptocurrency. Reasonable care would extend to safeguarding that property from obvious risks of harm – include cybersecurity threats.[177]

126 The Liquidators' reliance on cl 12 of the Terms and Conditions as a purported exclusion of general trustee duties[178] is also misplaced.[179] Moreover, there is a difference between whether a trustee has a

---

172 Liquidators' Submissions, [9.19]–[9.27].
173 Brocket I, 27 November 2019, TJSB1-11; [**401.0194**] at [**401.0211**].
174 Liquidators' Submissions, [8.197].
175 The Liquidators' Submissions articulate these propositions at [3.8].
176 *Ruscoe v Cryptopia Limited (in liq)* [2020] NZHC 728, [2020] 2 NZLR 809 at [184]; [**401.0365**] at [**401.0428**].
177 c.f. the Liquidators' Submissions to the contrary at [9.23].
178 Liquidators' Submissions, [9.27].
179 Primarily for the reasons articulated at [**269**]–[**344**].

duty and whether the trustee may be held liable for its breach. Further, despite its apparent breadth, cl 12 does not explicitly address trustee obligations. The law typically requires clear and express words to exclude such duties, which arise from the general law without needing to be articulated in the terms of the specific trust.[180]

127 Regardless of the above, and while the extent of Cryptopia's general duties as trustee is an interesting question, the specific issue of importance is of narrower compass. As is clear from GNY's creditor claim,[181] and from its notice of opposition to the Liquidators' Directions Application,[182] GNY's claim against Cryptopia as trustee is a claim for breach of *fiduciary* duty.

128 GNY's claim focuses the enquiry as to when a trustee's laxity can rise to the level of a fiduciary breach, as opposed to a species of negligence only.

129 Central to Cryptopia's trustee duties is its mandatory duty to act honestly and in good faith.[183] This duty has always formed part of the "irreducible core" of duties of all trustees:[184] its origin is in the fiduciary relationship of loyalty, and so is distinct from non-fiduciary duties of care. As the Liquidators properly accept, the duty to act honestly and good faith "must have been an obligation Cryptopia owed to its account holders: it forms the irreducible core of trustee obligations, and without it, there can be no trust".[185]

130 The key issue is, then, the scope of this duty required in the circumstances of this particular trust, and whether Cryptopia fulfilled those requirements. Much of the Liquidators' discussion in their submissions regarding the ambit or otherwise of Cryptopia's non-fiduciary duties does not engage with this key question.

---

180 See *Cooper v Pinney* [2024] NZSC 181, [2024] 1 NZLR 935 at [120].
181 See the draft amended statement of claim prepared by GNY and attached to its interlocutory application on notice by applicant for orders requiring confirmation of creditor claim under the Companies Act 1993, COA5.
182 See Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025, at [2.2(a)(i)] and [3.2]; [**101.0016**].
183 Trusts Act 2019, s 25.
184 *Armitage v Nurse* [1998] Ch. 241 (CA), [1997] 3 WLR 1046 per Millet LJ.
185 Liquidators' Submissions, [8.215].

131 It is now well established that a trustee's duties to act in good faith does not merely require a trustee to refrain from acting in bad faith. Rather, it may require a trustee to *positively act* in the interests of its beneficiaries.[186] A minimum level of focus and application is required for a trustee to discharge their fiduciary responsibilities. There is no disagreement between GNY and the Liquidators on this framing, as the Liquidators make the same point in their submissions.[187] In particular:

131.1 a decision that might otherwise appear to be open to a trustee can be impugned as a breach of the duty of good faith because of "a complete absence of applied thinking";[188] and

131.2 a trustee's omissions may be impugned as lacking in the requisite good faith because a trustee failed to "take active steps to protect beneficiaries' interests… particularly where the trustee knows of circumstances that could put those interests at risk of harm".[189]

132 Where situations of this kind arise, a trustee's discharge of the fiduciary duty of good faith, and performance of the general duty of reasonable care, may overlap. This is not because the duties collapse into each other as a matter of law: rather, it is because the trustee's very approach to their task – especially when they know of a real risk but run it anyway – can constitute a failure to act in good faith.

133 The recent decision of the Singaporean Court of Appeal in the *Ivanishvili* litigation illustrates this point, and provides useful guidance on when a trustee is required to take positive steps to protect beneficiary interests.[190] The Court elaborated the fiduciary good faith duty has having a positive dimension in the "adjectival" and "actuating" sense. The adjectival dimension attaches to or regulates the performance of non-fiduciary duties or exercise of

---

186 *Credit Suisse Trust Ltd v Ivanishvili* [2024] SGCA(I) 5 at [44]; see also Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [6.4.3(3)].
187 Liquidators' Submissions, [8.218]–[8.219].
188 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [6.4.3(3)].
189 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [6.4.3(3)].
190 *Credit Suisse Trust Limited v Ivanishvili* [2024] SGCA(I) 5.

powers, such as Cryptopia's exercise of its duty of reasonable care.[191]

134 The actuating dimension, importantly, focusses on when a trustee is *required* to act. In essence, a trustee is required to take positive, affirmative action in circumstances where it is known to the trustee that the interests of the beneficiaries are at risk of harm. [192]

135 The Court explained the actuating dimension of the good faith duty by illustration: a trustee stores gold bullion in an unsecured room left visible to passers-by. If the trustee watches a stranger remove gold bullion and does nothing, when the trustee knows the stranger is not a beneficiary and is not entitled to take the bullion, this conduct is "nothing short of disloyal".[193] It is distinct from a trustee who simply leaves the room and a theft occurs while the trustee is absent, or fails to lock the door, and a theft occurs without the trustee's knowledge.

136 The actuating dimension of a trustee's good faith duty therefore focusses on a trustee's state of mind: the first question is whether a trustee should have *acted* in particular circumstances given what the trustee knew, as opposed to whether a trustee achieved a particular outcome.[194] The second question is whether any actions actually taken by the trustee were *enough* in the circumstances. The decision in *Ivanishvili* illustrates that lackadaisical action by a trustee in the face of a known risk of harm will not be sufficient to discharge the actuating dimension of the good faith duty.[195]

137 In performing its good faith duty, Cryptopia needed to have regard to the context and objectives of the trust.[196] That is because it is

---

191 *Credit Suisse Trust Limited v Ivanishvili, Bidzina and others* [2024] SGCA(I) 5 at [47].
192 *Credit Suisse Trust Limited v Ivanishvili, Bidzina and others* [2024] SGCA(I) 5 at [48].
193 *Credit Suisse Trust Limited v Ivanishvili, Bidzina and others* [2024] SGCA(I) 5 at [52].
194 *Credit Suisse Trust Limited v Ivanishvili, Bidzina and others* [2024] SGCA(I) 5 at [48].
195 In the case, an unauthorised person removed millions of Euros from a trust account over an extended period. The trustees wrote a number of letters to the unauthorised person seeking explanations for the transfers, but the Court held this action was desultory and insufficient to discharge the trustees' obligation to act: *Credit Suisse Trust Limited v Ivanishvili* [2024] SGCA(I) 5 at [19].
196 This is not codified in s 21 of the Trusts Act 2019.

elementary trust should be administered in a way that is consistent with its purposes.[197] Relevantly to the objectives of the LML Trust:

137.1 Cryptopia required GNY to register a user account on the Cryptopia platform as part of its requirements for GNY to list LML as a new proprietary trading token on the Cryptopia trading platform.[198] LML was listing on the Cryptopia exchange for the first time. Its new listing facilitated trading in LML among a closed ecosystem of Cryptopia account holders to whom Cryptopia owed fiduciary duties. It was not (absent a hack) possible to remove the token from the Cryptopia exchange. This is the context in which Cryptopia's trustee obligations concerning LML held in its accounts were formed.

137.2 Cryptopia understood that LML was a new proprietary token launching on its platform.[199] GNY was the initial trust settlor.

137.3 A key objective of the trust was not merely the trading of cryptocurrency for profit generally, but specifically the successful launch of a market for the LML token. Cryptopia facilitated LML trading on the exchange, including by monitoring and publicising prices for the LML token, and establishing and safeguarding the LML wallet, the contents of which it held in its capacity as trustee.[200]

137.4 The safety and security of the Cryptopia platform, and specifically its wallet environment, was, at all times, essential to purpose of the trust and the capacity of the trustee to deliver on the trust's objectives – whether those objectives are construed as narrowly as holding beneficiary coins and acting on the direction of that beneficiary as a bare trustee, or more broadly in the context of LML's listing as a new token on the exchange. This was known and understood by Cryptopia. It actively promoted its exchanges to users as

---

197 See, for example, s 4 of the Trusts Act 2019.
198 [redacted] 31 March 2025, at [10]–[11]; [**201.0001**] at [**201.0003**].
199 [redacted] 31 March 2025, at [10]–[11]; [**201.0001**] at [**201.0003**]. See also [redacted] description of the proposed launch to Cryptopia, advising GNY will be "very pleased if we can have Cryptopia as our first exchange": Sibenik I, 1 August 2025, PJS1-90.
200 [redacted] 31 March 2025, at [10]–[12]; [**201.0001**] at [**201.0003**].

"safe" and "secure" – both on its website, and in its Terms and Conditions.[201] Both features were intrinsic to the services that GNY provided: cybersecurity is an essential feature of the ability to hold coins (and withdraw or trade at the beneficiary's request) on any cryptocurrency exchange. Cyberattack was a well-known, and well-understood, industry risk.[202]

138 It is against that background that GNY says that Cryptopia's fiduciary duty of good faith was engaged, and not discharged. More specifically, GNY relies on Cryptopia's:

138.1 knowledge of the *specific risk* of the Hack occurring;

138.2 knowledge of the *inadequacy and unacceptability of its security posture*; and

138.3 its *near total failure to do anything* to address these known risks before the Hack took place.

139 These are, of course, matters of fact. Together, they establish Cryptopia's breach of the good faith duty articulated in *Ivanishvilli*.

Cryptopia was specifically warned about the Hack

140 Cryptopia was warned by the New Zealand Government, through the GCSB, that Cryptopia's cryptocurrency trading platform was an identified target of state-sponsored cyber-attackers. These are the attackers who are suspected of ultimately undertaking the Hack.[203]

141 The GCSB warned Cryptopia of this threat in March 2018, nearly a year before the Hack occurred.[204] The GCSB contacted Cryptopia's senior management, including directors Rob Dawson and

---

201 [redacted] 19 December 2025, at [62]–[65]; [**201.0141**] at [**201.0153**].

202 Dicks I, 18 December 2025, at [30]–[34]; [**201.0154**] at [**201.0164**] to [**201.0165**]. Mr Watson agrees: Watson I, 31 July 2025, at [12]; [**201.0072**] at [**201.0075**].

203 Mr Watson suggests the attackers are affiliated with North Korea: Watson I, 31 July 2025, at [46]; [**201.0072**] at [**201.0082**].

204 Dicks I, 18 December 2025, at [45]; [**201.0154**] at [**201.0170**] to [**201.0171**], see also Ruscoe I, 31 July 2025, at [73]; [**201.0023**] at [**201.0043**] and DIR2-200 – 201; [**201.0117**] at [**301.0072**] to [**301.0073**].

Adam Clark, directly about this imminent threat, and was sufficiently concerned to meet with them to convey its gravity.[205]

142 Cryptopia was not only generally aware of the importance of cybersecurity to users of its platform, it was also specifically made aware – by a credible, informed and expert source – of the specific risk that ultimately manifested in the Hack. Cryptopia was, as trustee, on notice of a specific risk to trust assets. The focus is therefore firmly on what Cryptopia did, in light of that knowledge, to actively protect trust assets under its care.

Cryptopia knew that its cybersecurity posture was inadequate

143 Cryptopia's actions have to be assessed against a second strand of knowledge, concerning vulnerabilities of Cryptopia's system. Here, the evidence is also clear: Cryptopia had detailed and uncomfortable knowledge of its own cybersecurity vulnerability for well over a year before the Hack occurred – including at the time it was warned by the GCSB that it was an identified hack target.

144 There are three indicators that Cryptopia was aware, at all relevant times, that its cybersecurity settings were seriously lacking.

145 First, Cryptopia was warned repeatedly that it was vulnerable to cyberattacks by its external cyber-security advisors, Pulse. Pulse advised Cryptopia that it needed to take serious and immediate corrective steps to improve its cyber-security.

146 Mr Dicks correctly described the issues which Pulse identified in its testing and reporting to Cryptopia as systemic, and indicative of a culture of lax cyber-security.[206] It is clear from Mr Dicks' assessment that Pulse raised similar and repeated concerns about basic security failings at Cryptopia over the course of nearly a year.[207] The Pulse reports do not detail corrective action taken by Cryptopia: the reports are diagnostic and recommendatory, not remedial.

---

205 See Ruscoe I, 31 July 2025, DIR1-349; [**201.0023**] at [**301.0361**], see also [73]–[74]; [**201.0023**] at [**201.0043**] to [**201.0044**].
206 Dicks I, 18 December 2025, at [55]; [**201.0154**] at [**201.0173**].
207 Dicks I, 18 December 2025, at [55]; [**201.0154**] at [**201.0173**].

147 The second indicator of Cryptopia's knowledge of its vulnerability to a cyberattack are the warnings it received from its most senior technical staff. Those warnings were issued in plain, and unmistakable, terms by Morgan Nicholson, Cryptopia's Operations Manager in 2018.

148 In his evidence, Mr Ruscoe describes Mr Nicholson as follows:[208]

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

149 Mr Ruscoe also states in connection with Mr Nicholson that "Cryptopia management had clear responsibilities, but that this was frequently overridden or ignored by Cryptopia's founders/directors".[209] This observation is borne out in the warnings Mr Nicholson provided about the abysmal state of Cryptopia's cyber-security. The unmistakable picture is of an organisation well out of its depth, having taken on safeguarding responsibilities it was not prepared to handle.

150 For an example, see Mr Nicholson's email of 24 February 2018, sent shortly after Pulse identified that Cryptopia was using default "admin" credentials on its external firewall, and received by (among others), Cryptopia director Rob Dawson and CEO Alan Booth. By this time, Pulse had already identified serious vulnerabilities across all facets of Cryptopia's platform, and Cryptopia had repeatedly failed basic penetration tests. In his email, Mr Nicholson:[210]

150.1 Outlined that Cryptopia had failed Pulse's penetration tests, and explained that Pulse "have proven that easily, they can breach our security, get DB and wallet access, and thus easily have taken everything not in cold storage – they have done this 3 times now, utilizing 3 different vectors of attack… our networks and staff in Chch/UK are extremely vulnerable and no systems exist to prevent anything from happening once a hostile entity is in the inside – to assume that we are not the target of sophisticated attacks would be extremely foolish, so

---

208 Ruscoe I, 31 July 2025, at [82(b)]; [**201.0023**] at [**201.0046**].
209 Ruscoe I, 31 July 2025, at [82]; [**201.0023**] at [**201.0046**].
210 Ruscoe II, 4 November 2025, DIR2-297; [**201.0117**] at [**301.0474**].

to have this vulnerabilities ongoing without plans to do something about it is of critical importance".

150.2 Explained that Mr Nicholson felt "hamstrung" by management that "this is an issue that is really even worth discussion", going on to explain that the risk of a cyberattack and material theft of cryptocurrency "should stop all of you from being able to sleep at night, because your job security with Cryptopia is extremely dependant on a department of this company which I would describe as extremely neglected and in crisis".

150.3 Expressed frustration at management's efforts to slow or stop efforts to engaging Pulse, and expressed serious concern that his department was understaffed, and he was significantly overworked, and had insufficient capacity to manage risks associated with network changes and developments.

151 It appears that, by around June 2018, Cryptopia's directors and senior managers had excluded Cryptopia's most senior technical staff from its senior leadership team, including Mr Nicholson, and Mr Oakes, who was appointed as Cryptopia's Infrastructure Manager in May 2018.[211] This occurred despite Cryptopia senior management and directors' awareness that Cryptopia was an identified target of state-sponsored hackers – and knowledge that Cryptopia's cybersecurity settings made it "extremely vulnerable" to an attack of exactly this kind. Management did not want to hear what Cryptopia's technical staff were telling them.

152 Mr Nicholson's 8 August 2018 email to Cryptopia director Peter Dawson warned of some of the concerning consequences of Cryptopia's decision to remove technically expert staff from senior leadership discussions. In his email, Mr Nicholson:[212]

152.1 Repeats his concerns about "why a lack of IT governance has continued for so long and still remains largely unaddressed".

---

211 See, by way of example Ruscoe II, 4 November 2025, 28 May 2018 management team meeting minutes include Mr Nicholson and Mr Oakes, Cryptopia's senior technical managers: DIR2-309; [**201.0117**] at [**302.0507**]. By June 2018, Mr Nicholson and Mr Oakes were excluded from those meetings: DIR2-317; [**302.0593**] at [**302.0595**]. Mr Oakes was employed by Cryptopia between May and December 2018: Watson I, 31 July 2025, at [15]; [**201.0072]** at [**201.0076**].

212 Ruscoe II, 4 November 2025, at DIR2-329; [**201.0017**] at [**302.0615**].

152.2 Reiterates that those concerns arise as a result of the exclusion of Mr Nicholson and Daniel Oakes from the senior leadership team: "… there are 0 technical 'Senior Managers' within the business". Mr Nicholson describes this as "especially insane in a Tech company" and this results in technical leaders (such as himself) being "told to shut up and do".

152.3 States his concern that "[n]on-technical leaders of the business are circumventing technical leaders of the business, knowing that we will object and raise concerns, but those objections are seen as unacceptable delays instead of valid and reasonable technical objections".

152.4 Requests the implementation of policies to ensure that IT risks raised by technical leaders cannot be overruled by non-technical staff "including the General Manager and CEO".

153 The third indicator that Cryptopia was aware that its cybersecurity settings were manifestly inadequate, and insufficient to repel the cyberattack the GCSB had warned was coming, is found in an exchange Cryptopia had with the Financial Markets Authority (**FMA**) around March 2018.

154 It appears that, around March 2018, the FMA had engaged with Cryptopia regarding "concerns we have previously raised".[213] These concerns appear to include some FMA concerns about Cryptopia's disclosures to account holders,[214] as well as least four complaints received by the FMA about unauthorised access to personal wallets.[215] Sometime around March 2018, the FMA requested that Cryptopia directors provide an "attestation" expressed in the following terms:[216]

> Cryptopia:
>
> - has, based on accepted business risk, arrangements, systems, processes and controls ('Processes') in place to protect Cryptopia against malicious online attacks and that it takes appropriate steps

213 Ruscoe II, 4 November 2025, at DIR2-345; [**201.0017**] at [**301.0367**].
214 Ruscoe II, 4 November 2025, at DIR2-348 – 349; [**201.0117**] at [**301.0443**].
215 Ruscoe II, 4 November 2025, at DIR2-345 – 347; [**201.0117**] at [**301.0367**].
216 Ruscoe II, 4 November 2025, at DIR2-350; [**201.0117**] at [**301.0445**].

> to ensure those Processes operate effectively, including ongoing testing and continuing review of those Processes.
>
> - has never been successfully hacked.

155 Cryptopia's directors ***declined*** to provide the requested undertaking to the FMA. The reason provided to the FMA for that refusal was that "because it is continuing to improve its security measures, the directors *cannot attest to the current state adequacy as requested*" (emphasis added).[217]

156 Instead, Cryptopia agreed to provide a letter to the FMA "setting out the views of management and its Board regarding the adequacy of its current security processes".[218]

157 The letter Cryptopia provided to the FMA appears to have been sent to the FMA around late April 2018. It was signed by director Rob Dawson and expressed in the following terms:[219]

> Cryptopia has invested and continues to invest significant funds and resources in continuously reviewing and improving security measures to protect Cryptopia systems against potentially malicious online attacks.
>
> Security is of core concern to Cryptopia, particularly given the industry and the amounts of cryptocurrency held in our wallets. Security is a continual process, Cryptopia regularly have external security specialists conduct testing on our systems and provide recommendations for improvements to our systems and processes.
>
> As far as we are aware, Cryptopia has never been successfully hacked from a malicious external party.

158 Mr Dawson's letter to the FMA was, at the very least, misleading by omission. Cryptopia had in fact been successfully hacked on at least three occasions between November 2017 and February 2018 - by Pulse, a service provider tasked with *simulating* a malicious external attack. There is nothing to suggest that Cryptopia disclosed to the FMA that:

158.1 Its external and internal technical advisors had raised very recent and serious concerns about Cryptopia's material cybersecurity vulnerabilities in very strong terms.

158.2 It had ***not***, in fact, implemented the recommendations made by its external security specialists following its very poor

---

217 Ruscoe II, 4 November 2025, at DIR2-350; [**201.0117**] at [**301.0445**].
218 Ruscoe II, 4 November 2025, at DIR2-352; [**201.0117**] at [**301.0447**].
219 Ruscoe II, 4 November 2025, at DIR2-357; [**201.0117**] at [**301.0001**].

penetration testing performances (as we explain in more detail below).

158.3 Its governance structures and management culture were trending against, rather than towards, the focus and investment required to correct its security vulnerabilities.

158.4 It was at risk of an imminent and significant attack, and had been specifically warned of this fact by GCSB, and was advised to take implement at 24/7 monitoring services – but had neither actually done so; nor put in place any other serious or credible plans to address the coming risk.

159 What is clear from this exchange is that as at April 2018, Cryptopia's directors were unprepared to confirm the adequacy of their cybersecurity state to the FMA – because they actually knew that state was not, in fact, adequate.

160 Pausing here, Cryptopia was obviously on notice of a specific and serious threat to coins on its platform. When it was put on notice of that threat by the GCSB, it was already aware that its platform was highly (and unacceptably) vulnerable to the risk in question. As a trustee, acting in good faith, Cryptopia was obligated to take steps to protect beneficiaries' interests, including proactively implementing and maintaining appropriate safeguards and security arrangements.

Cryptopia did not address its cybersecurity vulnerabilities

161 Cryptopia did not, however, take action to address the cybersecurity failings identified by Pulse.

162 While the Liquidators have suggested in their submissions that Cryptopia did have *some* cybersecurity,[220] and did *try* to address its vulnerabilities,[221] the available evidence strongly suggests that Cryptopia did not in fact respond appropriately – or indeed, take any

---

220 Liquidators' Submissions, [8.111]–[8.113]. Note, however, these submissions appear to overstate the position: several of the items referred to are not cybersecurity measures, or relevant to the vulnerabilities identified by Pulse: see discussion at [**92.1**] below.

221 Liquidators' Submissions, [8.124].

material action – to address the cybersecurity vulnerabilities identified by Pulse.

163 There are three sources of information that, taken together, strongly suggest that Cryptopia did not take steps to address the serious vulnerabilities identified in the Pulse reports before the Hack occurred in January 2019.

164 First, information sourced by the Liquidators from Cryptopia's directors and managers.

165 Arguably, this information source is the least useful of the three available to the Court. This is because Mr Ruscoe's evidence on this topic provides no more than high level summaries of potentially relevant comments from directors and managers in s 261 interviews.[222] Without being placed in context and tested, this second-hand information must be treated with great care. Cryptopia's management is obviously motivated to justify and defend its own actions. And what matters in a case like this is not general blandishments, but specific answers to forensic questions.

166 Yet the Liquidators have declined to disclose the transcripts of those interviews,[223] have not provided the questions that the Liquidators asked of the managers and directors in question, and have not explained what information those managers or directors were shown to comment on. GNY is not, of course, able to cross-examine those individuals, and in most cases, has not been told who actually made the comment in question, or when. There is also surprisingly little information available from those interviews about Cryptopia's

---

222 See Ruscoe I, 31 July 2025, at [60]–[85]; [**201.0023**] at [**201.0040**] to [**201.0047**].

223 GNY requested (among other matters) copies of extracts of the s 261 transcripts which led to the matters Mr Ruscoe describes in his evidence on cybersecurity matters, and any other extracts from those transcripts including "questions and answers about the Hack, the cause of the Hack, or Cryptopia's response to the Hack, or the nature of Cryptopia's arrangements, the adequacy of those arrangements or security planning; or discussion or risks to the exchange" (CT-BF letter, 20 August 2025). The Liquidators declined this request on the surprising basis that "purpose of the s 261 interviews was broadly to provide the liquidators with the knowledge of the Company's affairs that would have been held by directors and senior management, and the transcripts are held by the liquidators and not by Cryptopia. The liquidators consider that GNY's claims fall outside of the scope of that purpose, and it would not be appropriate to provide copies of those transcripts or extracts of them." (BF-CT letter, 27 August 2025).

cybersecurity posture, given Cryptopia's liability for the Hack was always going to be relevant to the position of Hack victims like GNY.

167 It is, in any event, apparent from Mr Ruscoe's evidence that:

167.1 Cryptopia did not have a dedicated in-house security team.[224]

167.2 While Cryptopia management told the Liquidators that they "took steps" to implement improved security measures "regarding password security and Cryptopia's domains" in response to the Pulse reports, these purported improvements were "ad hoc" and it is not clear that "all of the recommendations were implemented".[225]

167.3 It is not even clear from Mr Ruscoe's evidence what these purported steps to improve security measures actually were. It appears the directors and managers interviewed by the Liquidators provided no concrete information to the Liquidators on any specific security improvement measure.[226] This lack of relevant details reflects Cryptopia's documentary records, which do not identify any specific remedial actions either (as explained below). It is difficult to see how much, if any weight could be placed on generic claims from unidentified persons that Cryptopia "took [unexplained] steps" to improve cybersecurity.

167.4 There is nothing in the comments which Cryptopia managers or directors made to the Liquidators to suggests that Cryptopia took any steps at all to address the most significant cybersecurity deficiencies identified by Pulse in its reporting: for example, addressing Cryptopia's total lack of any meaningful network segregation, or addressing its seriously lax administrator access privileges including access to wallet keys.[227]

---

224 Ruscoe I, 31 July 2025, at [69]; [**201.0023**] at [**201.0042**].
225 Ruscoe I, 31 July 2025, at [76]; [**201.0023**] at [**201.0045**].
226 See similarly vague and unclear comments in Mr Ruscoe's 4 November 2025 affidavit, at [9]–[30]; [**201.0117**] at [**201.0119**] to [**201.0125**].
227 See Ruscoe I, 31 July 2025, at [60]–[85]; [**201.0023**] at [**201.0040**] to [**201.0047**].

167.5 There was considerable debate among Cryptopia directors and senior managers on whether to engage Pulse to address the cybersecurity deficiencies it identified, or TSS Datacom, or PwC, or another provider.[228] However, none of the comments made by managers or directors to the Liquidators suggest Cryptopia actually implemented changes to address cybersecurity deficiencies. It is apparent from the s 261 interview material provided that Cryptopia did not even adopt the GCSB's primary recommended security step (24-hour monitoring) after it specifically warned Cryptopia of a likely future cyberattack.[229] This internal debate makes clear that the interviewed managers and directors were certainly *aware* of the need to do something to address cybersecurity vulnerabilities. But it does not suggest they actually did anything relevant at all.

167.6 While Mr Ruscoe's evidence suggests that Cryptopia's internal debate at least in part related to whether a comprehensive strategic review needed to be undertaken before taking steps to fix known and serious cybersecurity vulnerabilities,[230] it is apparent that Cryptopia did not actually progress any such review[231] - and the contemporaneous records suggest there were other reasons for not taking steps to address cybersecurity matters.[232] As is explained below, it appears

---

228 Ruscoe I, 31 July 2025, at [73]–[84]; [**201.0023**] at [**201.0043**] to [**201.0046**].

229 Ruscoe II, 4 November 2025, at [29]; [**201.0117**] at [**201.0125**]. Note that, as Mr Dicks points out, GCSB may not have been aware that Cryptopia's basic security settings were seriously deficient when it made its recommendations: Dicks I, 18 December 2025, at [47]; [**201.0154**] at [**201.0171**].

230 Ruscoe I, 31 July 2025, [78]; [**201.0023**] at [**201.0044**].

231 Mr Ruscoe's evidence attaches discussions with Datacom TSS in early to mid-2018 about procuring a "Security Posture Snapshot" which Cryptopia appeared to show some interest in. However, it clear from Cryptopia's records that (notwithstanding insistence from a senior technical staff member), Cryptopia did not engage with Datacom TSS to complete this review: see Ruscoe I, 31 July 2025, DIRI-347; [**201.0023**], [**301.0359**] and Ruscoe II, 4 November 2025, DIR1-278-283, in particular DIR1-280; [**201.0117**], [**302.0671**]–[**302.0676**], [**302.0673**]. This is consistent with Mr Ruscoe's advice that Cryptopia did not proceed with contracts to fix with any of Datacom TSS, Kordia or Pulse: Ruscoe I, 31 July 2025, [78]; [**201.0023**] at [**201.0044**].

232 In fact, the suggestion that some (unnamed) managers or directors believed a "comprehensive strategic review" was needed before taking steps to fix known security vulnerabilities is a surprising claim, given that the initial Pulse "Consulting Summary" Report in 2017 was in the nature of a one week review of Cryptopia's full operating environment and configurations, for the purposes of making recommendations on the level of security: see Pulse "Consulting Summary", November 2017, Ruscoe I, 31 July 2025, DIR1-111; [**201.0023**], [**301.0137**]. The contemporaneous records suggest that the primary focus of senior executives /

from Cryptopia's records that Cryptopia chose not to proceed with cybersecurity fixes as it wished to prioritise spending on other matters.

167.7

168 The second source of information is Cryptopia's documentary comments on cybersecurity measures taken through the course of 2018.

169 These records mostly take the form of Pulse reporting, which was diagnostic not remedial – together with a draft IT infrastructure plan prepared around May 2018, which was primarily directed to infrastructure build, and which did not address the identified the cybersecurity vulnerabilities identified by Pulse; possibly because the report itself suggests that the author (a very new staff member at the time) was not actually provided with the Pulse reports.[233] There is no evidence that the draft IT infrastructure plan was finalised, let alone implemented.

170 The last substantive internal update on Cryptopia's cybersecurity settings before the Hack is informative. It is a 24 October 2018 cybersecurity update from its "virtual CISO", an employee of Pulse on part-time secondment to Cryptopia for three months beginning in July 2018.[234]

171 That report confirms that, despite knowing for close to a year by this stage that its cybersecurity posture rendered it highly vulnerable to cyberattacks, and despite knowledge of a specific planned attack, Cryptopia's cybersecurity posture remained inadequate. The report records that, as of October 2018, less than three months before the Hack:[235]

171.1 Cryptopia's purpose in employing a "virtual CISO" was to help ensure Cryptopia could withstand sophisticated cyber-attacks;

---

directors at the time may have actually been a reluctance to spend on security measures: see Ruscoe II, 4 November 2025, DIR2-292; [**201.0117**], [**301.0266**].

233 See Mr Dicks' summary of this document: 18 December 2025, at [56]–[75]; [**201.0154**] at [**201.0174**] to [**201.0179**].

234 See Ruscoe II, 4 November 2025, DIR1-320 – 321; [**201.0017**] at [**302.0598**] to [**302.0599**].

235 Ruscoe I, 31 July 2025, DIR1-345; [**201.0023**] at [**302.0729**].

171.2 however, while Cryptopia's cybersecurity had improved (in unexplained ways, and against a very low baseline), "limited" progress had been made against the goal of helping Cryptopia withstand cyberattacks;

171.3 this appears to be because of a "lack of strong direction from the board or SLT" on cybersecurity, and the "lack of prioritisation of resources towards security improvements". This damning observation is, of course, consistent with Mr Nicholson's emails raising serious concerns about senior management's / directors' lackadaisical approach to significant cybersecurity needs. These records together provide the best available explanation for why none of the various cybersecurity improvement options explored by Cryptopia staff between February and March 2018 were ever actually acted on;

171.4 around 50% of "fundamental security controls" were "missing", with the other 50% mostly – but not entirely – implemented. A house which has half of its doors closed and locked is still 100% at risk of being burgled;

171.5 alarmingly, Cryptopia could not yet repel attacks such as those simulated by Pulse's November 2017 and February 2018 penetration testing – despite those tests resulting in complete compromise of the platform using relatively unsophisticated techniques, and identifying fixable vulnerabilities; and

171.6 overall, Cryptopia's cybersecurity stance was "weaker than reasonably required of a Cryptocurrency exchange" and "far from the level of security maturity required for a cryptocurrency exchange".

172 Appointing a short-term, part-time virtual CISO – whilst not providing that person with the resources or support necessary to implement measures required to actually address Cryptopia's known vulnerability to a cyber-attack – was desultory, and entirely insufficient to discharge Cryptopia's obligation as trustee to take action to address a known and specific risk to trust assets. The picture that emerges is that Cryptopia actively *chose* not to

prioritise addressing this known risk in favour of other commercial priorities.

173 Relevantly:

173.1 Cryptopia had access to the resources which it could have used to improve its cybersecurity posture through the majority of 2018. For example, its June, August and September 2018 balance sheet consistently show that Cryptopia held between $17,000,000 and $24,000,000 of liquid assets (cash or cryptocurrency), and stable retained earnings of around $24-25,000,000;[236]

173.2 the Liquidators' expert has suggested that addressing the issues raised in Pulse's reports would cost a minimum of $200,000-$400,000, and take three to six months.[237] Cryptopia had well more than that amount on hand, in cash, when it was first advised of its major vulnerabilities, when it failed basic penetration tests, when it was warned by GCSB, and when its directors refused to attest to current state adequacy at the request of the FMA; and

173.3 throughout this period, Cryptopia continued to advertise its platform on its website as safe and secure, including to GNY.[238] GNY listed the LML token on the Cryptopia exchange in November 2018 - shortly after the virtual CISO report confirmed that Cryptopia still fell well short of the expected cybersecurity standards of a cryptocurrency exchange.

174 The third source of information is Mr Dicks' systemic review of Cryptopia records to identify any indicators in those records that may confirm whether Cryptopia took the necessary technical steps to address the material deficiencies in its cybersecurity posture before the Hack occurred in January 2019.

175 As Mr Dicks explains:[239]

---

236 Ruscoe I, 31 July 2025, DIR1-371 – 375; [**201.0023**] at [**302.0543**; **302.0602**; **302.0603**; **302.0679** – **302.0682**].
237 Watson II, 28 January 2026, at [8]; [**201.0252**] at [**201.0254**].
238 See [redacted] 19 December 2025, at [62]–[65]; [**201.0141**] at [**201.0153**].
239 Dicks I, 18 December 2025, at [64]–[75]; [**201.0154**] at [**201.0175**] to [**201.0180**].

175.1 Cryptopia's internal reporting, and Pulse reporting, suggests that Cryptopia's major cybersecurity deficiencies were not addressed. This is both because of express statements in those reports (such as those in the October 2018 virtual CISO report quoted earlier), and because Pulse's diagnostic reports repeatedly identify the same weaknesses over the course of nearly a year – the obvious implication is that Cryptopia's core cyber-security vulnerabilities had not been dealt with, and were not being dealt with;

175.2 he did not identify any documents which suggest Cryptopia undertook further penetration testing after it failed Pulse's initial testing, despite Pulse recommending that further tests occur - and despite industry practice being to repeat failed penetration tests, and document the fixes taken to address known vulnerabilities.[240] None of that paperwork exists. The obvious and likely reason why not is because the testing did not actually occur; and

175.3 nor did Mr Dicks identify any statements of work or invoices which suggest Cryptopia undertook the fixes recommended by Pulse. If that work had been undertaken, it is likely that at the very least a record of payment for that work would exist. But there are no such records to be found.

176 Overall, these sources of information strongly suggest that Cryptopia decided not to invest in addressing its cybersecurity vulnerabilities, despite knowing how severe those vulnerabilities were, and despite knowing of a specific risk of serious cyber-attack against its platform. Its decision not to act in those circumstances was disloyal, and a breach of its good faith duty to its beneficiaries.

177 Applying the illustration explained by the Court in *Ivanishvili* to Cryptopia's conduct before the Hack occurred, Cryptopia:

177.1 knew a stranger was on the way to take the gold bullion; and

---

[240] And, despite Cryptopia's assurances to the FMA that it undertook regular testing of its systems: see [**157**] of these submissions. In fact, the available evidence suggests that the last penetration testing Cryptopia completed was in February 2018. It did not undertake any further testing after its letter of assurance to the FMA in April 2018.

177.2 knew that the door the room containing the gold bullion was unlocked and so could be entered by the stranger easily all the while advising beneficiaries that the room was "safe" and "secure", and thus attracting more bullion into its safekeeping); but

177.3 did not get up and lock the door.

178 This was a breach of Cryptopia's duty to act in good faith as trustee.

Cryptopia's breach: post-hack

179 Furthermore, after the Hack, when Cryptopia knew that the "gold bullion" – actually highly valuable cryptocurrency - had been taken, it did not make any adequate efforts to retrieve it. This is despite Cryptopia knowing where the stolen LML tokens were held, and despite there being a very simple steps it could take in order to secure the stolen LML for retrieval by its rightful owner.

180 The evidence establishes that:[241]

180.1 for a period of time after the Hack, the stolen LML was traceable to an identifiable wallet on Bitbay;[242]

180.2 GNY, having traced its stolen LML to Bitbay, requested Bitbay to freeze the wallet containing the stolen LML. Bitbay did temporarily freeze the stolen tokens at GNY's request;[243]

180.3 however, Bitbay advised GNY that it could only permanently freeze the wallet containing the stolen LML in question if ***Cryptopia*** confirmed the theft of the LML from its exchange;[244] and

180.4 yet – despite multiple requests from GNY that it do so, and despite Bitbay contacting Cryptopia to request confirmation

---

241 See generally Dicks I, 18 Dec [redacted]025, at [91]–[93]; [**201.0154**] at [**201.0184**] to [**201.0185**], [redacted] 19 December 2025, at [22]–[29]; [**201.0141**] at [**201.0145**] t[redacted]**0147**] and the primary correspondence attached to the affidavits of Mr Sibenik at PJS1-92 – 95; [**302.0895**] to [**302.0897**], [**302.0892**] and [redacted] 30 March 2025, at [redacted]9 – 50; [**201.0001**] at [**302.0865**] to [**302.0894**].

242 See Sibenik I, 1 August 2025, at [65]; [**201.0090**] at [**201.0108**]; [redacted] 31 March 2025, at [16]; [**201.0001**] at [**201.0004**].

243 [redacted] 31 March 2025, at [16]; [**201.0001**] at [**201.0004**].

244 [redacted] 31 March 2025, at [16]; [**201.0001**] at [**201.0004**], and see also Sibenik I, 1 August 2025, PJS1-95; [**201.0090**] at [**302.0892**].

that the LML had been stolen in the Hack – Cryptopia did not take the simplest of actions to contact Bitbay and confirm the theft of LML.[245]

181 Had Cryptopia taken the simple steps necessary to permanently freeze the stolen LML, this would have facilitated the eventual return of those assets to GNY. More immediately, it would have allowed GNY to confidently and factually assure its investors and traders that no stolen coins were in circulation and tainting trading – an issue which caused GNY considerable difficulty in trying to contain the damage to LML's value arising from the Hack.[246]

182 The Liquidators' approach to this sequence of events in their submissions fails to engage with the pertinent facts. They point to various general actions taken by Cryptopia after the Hack, and suggest that means Cryptopia was "taking steps in the interest of all beneficiaries as a whole".[247] The Liquidators primarily mean Cryptopia was doing things to restore its exchange generally, as well as assisting the Police. While restoring the Cryptopia exchange may benefit those trusts which retained assets on that exchange after the Hack, it was of no real assistance to beneficiaries of hacked trusts like the LML trust.

183 With regard to the LML trust (which had nearly all of its property stolen in the Hack), the question to ask is what is required to discharge the good faith obligations of a trustee who (a) is the trustee of a trust (b) knows that a significant proportion of trust property has been stolen (c) knows where the stolen trust property is held and (d) has an specific opportunity – through a very basic step that has been requested of it by the trust's largest beneficiary – to permanently restrain the stolen trust property.

184 Focussing on facts relevant to Cryptopia's obligations as trustee of the LML trust, the Liquidators appear to have misunderstood what occurred. As [redacted] xplains in his evidence, Bitbay required

---

245 See, for example, [redacted] multiple emails to Cryptopia requesting that Cryptopia contact Bitbay to f [redacted] permanent freeze of stolen LML at Sibenik I, 1 August 2025, PJS1-92 – 95; [**302.0895**] to [**302.0897**], [**302.0892**].

246 See [redacted] 19 December 2025, at [9]–[15]; [**201.0141**] at [**201.0143**] to [**201.0144**], for a description of some of the difficulties arising from market confusion in the aftermath of the Hack.

247 Liquidators' Submissions, [8.231].

"formal verification from the authorities or the compromised exchange that the LML tokens were stolen property. Bitbay told us that it needed to be certain that it was lawful and appropriate for it to freeze the LML tokens permanently before taking that step, in order to protect Bitbay from any claims or allegations from the wallet holder. We were not in a position to provide the information Bitbay needed to freeze the stolen LML without Cryptopia's help".[248]

185 [redacted] evidence on this point reflects what GNY told Cryptopia about Bitbay's request at the time:[249]

> I emailed you earlier regarding the stolen LML tokens on Bitbay. Bitbay has confirmed that you have not contacted them at all about recovering them. Bitbay *cannot freeze wallets indefinitely without your and the NZ police's confirmation that these are stolen property.* Since then, more stolen LML tokens have arrived on Bitbay. We are now not able to sell our supply of LML tokens on Bitbay, and we have also informed our buyers to stop buying LML tokens from Bitbay, as we cannot be certain that these are not stolen tokens. These stolen tokens will now cause a further deterioration in the price and market capitalization of LML.
>
> (emphasis added)

186 The Liqudiators suggest in their submissions that GNY was able to, and did, provide Bitbay with this information, sourced from the NZ Police.[250] This claim is incorrect, as [redacted] evidence confirms: NZ Police were not in contact with GNY.[251] The Liquidators' stance also defies commercial commonsense: GNY desperately wanted its token frozen and returned. It just couldn't do so without Cryptopia's help:

186.1 GNY was only able to confirm to Bitbay that the Hack incident had occurred; which did not, of course, provide official third-party verification of any specific stolen tokens, nor verify the LML traced by GNY was the LML that had been stolen from

---

248 [redacted] 19 December 2025, at [26]; [**201.0141**] at [**201.0146**]. As [redacted] in his evidence, much of GNY's engagement with Bitbay was over chat function. The Liquidators' misunderstanding may arise because they have focussed solely on retained email correspondence with Bitbay, rather than [redacted] explanation of what occurred overall.

249 Sibenik I, 1 August 2025, PJS1-92; [**201.0090**] at [**302.0895**].

250 Liquidators' Submissions, [8.229].

251 [redacted] 19 December 2025, at [27]–[28]; [**201.0141**] at [**201.0146**] to [**201.0147**]. The Liquidators appear to have inferred that [redacted] provision to Bitbay of information from the NZ Police "acknowledging the incident" was information providing verification from the Police of the source of the stolen LML. Of course, NZ Police did publicly acknowledge the incident had occurred in statements to account holders published online: but this is a different matter to verification concerning stolen LML, and as [redacted] confirms, the Police were not in contact with GNY directly. See Sibenik I, 1 [redacted] 2025, PJS1-96; [**201.0090**] at [**302.0898**]. Therefore any such inference is unwarranted.

Cryptopia. Bitbay had requested verification that the LML tokens GNY had traced to its exchange were GNY's stolen property; and

186.2 only Cryptopia could provide the verification information, as it was the hacked exchange, and it was liaising with the New Zealand authorities.[252]

187 However – despite specific and repeated requests by GNY identifying the location of the stolen LML and requesting assistance – Cryptopia did not provide that assistance.

188 The scenario that arose here is again analogous to the illustration helpfully articulated by the Court in *Ivanishvilli*.[253] The LML trust trustee was aware of the location of stolen trust property. The trust property was plainly at specific, and immediate, risk. The trustee knew that there is a simple step it could take to address that risk. But the trustee did nothing.

189 Relevantly to whether Cryptopia's choice to do nothing was consistent with its good faith duty, recipient exchanges routinely freeze suspicious tokens if they are able to verify the tokens are likely to have been stolen.[254] A cryptocurrency exchange would typically have an incident response plan for engaging with accountholders to deal with requests of this kind.[255] So the scenario that arose with respect to the LML trust post-hack was not an unexpected or unpredictable scenario in the cryptocurrency industry: Bitbay's request for verification information was a typical industry request, and GNY's request to Cryptopia for that information is the sort of thing you would reasonably expect Cryptopia as trustee to have a plan in place to deal with.

Damages and fiduciary duty

190 Cryptopia's conduct breaches a core fiduciary obligation.

---

252 [redacted], 19 December 2025, at [26]–[27]; [**201.0141**] at [**201.0146**].
253 *Credit Suisse Trust Limited v Ivanishvili, Bidzina and others* [2024] SGCA(I) 5 at [52].
254 See Dicks I, 18 December 2025, at [92]–[95]; [**201.0154**] at [**201.0185**].
255 See Dicks I, 18 December 2025, at [92]–[95]; [**201.0154**] at [**201.0185**].

191 The Liquidators have appropriately acknowledged that Cryptopia's purported exclusion clauses can have no application to breaches of duties of this kind.

192 However, a further consequence follows. The courts have long recognised that breaches of fiduciary duties attract specific consequences, because of "the need to deter breaches of trust and confidence by those in a position to take advantage of the vulnerable by using powers to be exercised solely for their benefit".[256] This can mean that non-compensatory remedies arise (for example an account of profits), although that is not in issue in this case. Relevantly to the present case, it also means there is no fusion between the rules of common law and equity when considering questions of causation and remoteness arising from fiduciary breaches. The correct approach is:[257]

> …once the plaintiff has shown a loss arising out of a transaction to which the breach [of fiduciary obligation] was material, the plaintiff is entitled to recover unless the defendant fiduciary, upon whom is the onus, shows that the loss or damage would have occurred in any event, i.e without any breach on the fiduciary's part … Policy dictates that fiduciaries be allowed only a narrow escape route from liability based on proof that the loss or damage would have occurred even if there had been no breach.

193 In this case, Cryptopia's breach was, in fact, causative of GNY's loss.[258] That analysis applies with even more force to GNY's fiduciary breach claim.

---

256 *Bank of New Zealand v New Zealand Guardian Trust Co Ltd* [1999] 1 NZLR 664 (CA) at 681–682 per Gault J.

257 *Bank of New Zealand v New Zealand Guardian Trust Co Ltd* [1999] 1 NZLR 664 (CA) at 687 per Tipping J: subsequently endorsed by the majority of the Supreme Court in *Stephens v Premium Real Estate* [2009] NZSC 15, [2009] 2 NZLR 384.

258 See discussion of this below at [**227**]–[**239**].

Cryptopia's FTA breach

194 Cryptopia is also liable to GNY for misleading and deceptive conduct in breach of the Fair Trading Act 1986 (**FTA**).

The law

195 Cryptopia was indisputably in trade for the purposes of the FTA.

196 The approach to breaches of the misleading and deceptive conduct provisions in the FTA is well-established, but nonetheless flexible, and inherently fact and context-specific.

197 The Court must identify whether Cryptopia's conduct was misleading and deceptive. This test to be considered in all light of all the relevant facts and circumstances.[259] Generally, the Court will ask whether the conduct was capable of being misleading, before considering whether GNY was in fact mislead. These first two questions are essentially factual. The third step is to consider whether it was reasonable for GNY to be misled in all of the circumstances. This is an objective assessment, considered from the perspective of a reasonable member of the public considering the representations in question.[260]

198 Alternately, the Court may ask whether the claimant (in this case GNY) has demonstrated that a reasonable person its situation – e.g. with characteristics of which the defendant ought to have been aware – would likely have been misled or deceived. Any enquiry into loss or damage under s 43 follows.[261]

199 In this case, identifying the relevant cross-section of the public (or hypothetical reasonable persons with characteristics of the same nature as GNY) is straightforward: cryptocurrency traders on the Cryptopia platform.

200 Those traders were predominantly based offshore, and they were obliged to enter standard-form agreements with Cryptopia in order to use its platform (rather than negotiating bespoke terms). Such

---

259 See *AMP Finance NZ Ltd v Heaven* (1997) 8 TCLR 144.

260 *Red Eagle v Ellis* [2010] NZSC 20, [2010] 2 NZLR 492 at [22]. See also further clarification in *Godfrey Hirst NZ Ltd v Cavalier Bremworth Ltd* [2014] NZCA 418 at [43] per Wild J for the Court.

261 *Red Eagle v Ellis* [2010] NZSC 20, [2010] 2 NZLR 492 at [28]–[29] per Blanchard J for the Court.

traders would not be expected to be generally familiar with New Zealand law or regulation. While the Liquidators have suggested that GNY was legally represented in its engagement with Cryptopia,[262] that suggestion is incorrect, and there is no reason to think traders on the exchange typically sought legal advice in New Zealand generally before opening accounts with Cryptopia. Further, such persons would be reliant on the accuracy of Cryptopia's statements about its exchange, as they would have no capacity to interrogate those claims via independent enquiry: cybersecurity arrangements are internal management matters, and confidential, notwithstanding their critical importance to users of a platform like Cryptopia.

The Representations

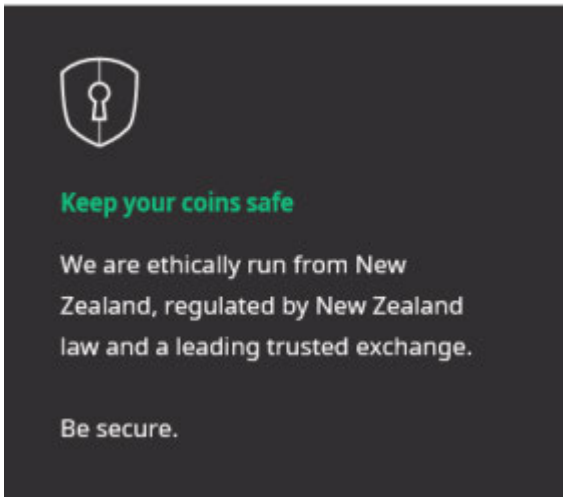
201 Section 9 of the FTA precludes persons in trade from engaging in conduct that is likely to mislead or deceive generally. Section 11 precludes conduct that is likely to mislead or deceive a person as the "nature, characteristics, [or] suitability for a purpose" of services. Section 13(b) of the FTA specifically precludes a person who is in trade from representing, in connection with the promotion or supply of services, that those services are "of a particular kind, standard or quality".

202 Cryptopia advertised itself on its website as follows:[263]

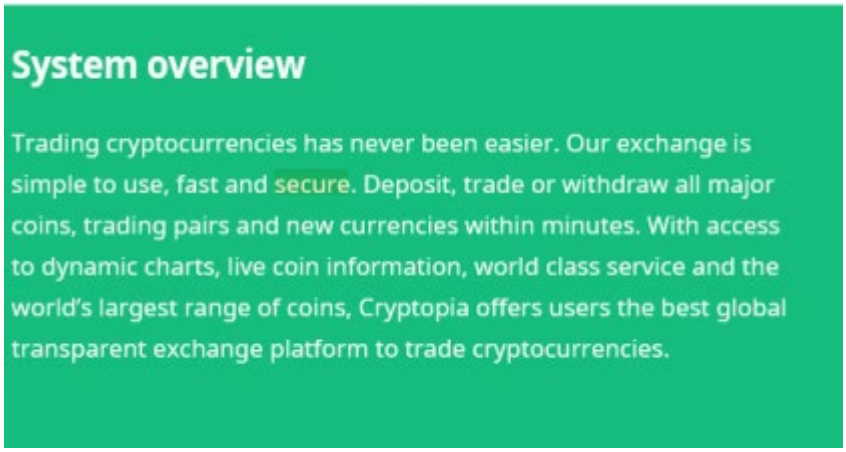
---

262 Liquidators' Submissions, [8.80]. As is apparent from the email which the Liquidators cite for this proposition, GNY was advised by Carey Olsen in respect of its initial coin offering in Jersey – [redacted] provides a link to Cryptopia with an article describing this engagement (see Sibenik I, 1 August 2025, PJS1-15). Carey Olsen is a law firm which operates in Bermuda, the British Virgin Islands, the Cayman Islands, Guernsey and Jersey – not New Zealand. It could not (and did not) advise GNY with respect to Cryptopia's terms. As is apparent from the full correspondence between GNY and Cryptopia, GNY engaged with Cryptopia directly through [redacted] at all times, and [redacted] is not legally trained.

263 [redacted] 31 March 2025, [redacted] 28; [**201.0001**] at [**301.0076**].



203 And as follows:[264]



(together, the **Representations**)

204 The Representations were made to induce cryptocurrency traders to use the Cryptopia trading platform. As an online exchange with an offshore client base, its website was its primary means of advertising.

205 The Representations are about the cybersecurity of Cryptopia's cryptocurrency trading platform. This is clear because:

205.1 The lock and key image, set immediately above a reference to "keep your coins safe" obviously implies that the coins on the exchange are protected from external malicious actors. In an

[264] [redacted] 31 March 2025, [redacted]28; [**201.0001**] at [**301.0076**].

online context, this must mean protected by appropriate cybersecurity measures.

205.2 This is reinforced by the reference to "be secure" and a "leading trusted exchange". To be "secure" is to be free from danger, fear, or threat.

205.3 The point is made expressly again in the second Representation: "our exchange is… secure".

206 Any reasonable reader of these statements would understand them as representations about the online safety and security of coins placed on the Cryptopia trading platform. Cybersecurity – and the risk of malicious online attacks – is the core safety and security concern for cryptocurrency trading platforms and traders who use them.[265] So this is the obvious and natural meaning of the Representations.

207 Representing that coins are "safe" and "secure" – under lock and key – will naturally bring to mind cybersecurity.

208 The Liquidators have suggested the Representations are "vague". To illustrate the point, the Liquidators point to four possible meanings – the safety and security of Cryptopia's website and web application, or account access, or account holder information and data, or Cryptopia wallets.[266] However, the proposition that these are distinct meanings indicative of vagueness is illusory: all four are examples of parts of Cryptopia's platform, or information or assets held on the platform, which could only be kept "safe" and "secure" through cybersecurity measures. Even then, the Liquidators' attempt to suggest ambiguity on the point ignores the specific reference to keeping "coins safe" in the first Representation, and the specific reference to the security of the exchange in the second, both of which direct the reader to the safety and security of customer assets held on the exchange.

209 Relatedly, the Liquidators suggest that the Representations are "puffery", by analogy to the statement "safe for the environment" – relying for this point on a decision concerning a criminal prosecution

265 Dicks I, 18 December 2025, at [34]; [**201.0154**] at [**201.0165**].
266 Liquidators' Submissions, [8.95].

in which the statement "safe for the environment" was not actually made, nor actually considered by the Court.[267] That decision is of no assistance. In any event, it is an unattractive commercial argument that an exchange platform's offer of a secure platform should be found to be meaningless and unenforceable, after it is relied on by users to their detriment.

210 Nor is the concept of puffery of any relevance to this case. "Puffery" is typically understood to be eulogistic style recommendations of the thing for sale, not capable of amounting to a representation.[268] The concept has never meant that representations which cannot be determined to be true or false by reference to a singular dispositive measurement standard are incapable of being a misrepresentation. If this approach to the FTA were correct, it would materially narrow the scope of the FTA from how it is routinely applied in practice. Misleading representations are often qualitative, or evaluative.[269] Context is everything. Again, claims of security on trading platforms cannot be regarded in law as idle boasts.

211 In this case, the Representations concern a specific and critical feature of the service Cryptopia offered, and the evidence clearly establishes that Cryptopia was very unsafe, and very insecure, when compared to any reasonable or appropriate cybersecurity stance for a cryptocurrency exchange.[270]

212 As noted above "secure" means to be free from threat. The only plausible read of the Representations is that coins on the Cryptopia exchange were safe and secure from the obvious and most prevalent external threat: cyberattack – whether as a result of the exchange being an "ethically run" exchange "regulated by

---

267 See Liquidators' Submissions, [8.97], citing *Commerce Commission v Eco-Pal Ltd* DC Auckland CRI-2010-063-4397, 21 June 2013 at [64]. The prosecution in question concerned representations regarding the biodegradability of plastic in landfill conditions, and one expert, in passing, is said to have mentioned in his evidence that comments such as "safe for the environment" are less likely to carry weight with consumers. The phrase was, in the context of the decision, a hypothetical one of no particular consequence, is not mentioned in the decision again, and plainly does not form part of the decision, including at [102].

268 John Burrows, Jeremy Finn, Stephen Todd *Burrows, Finn and Todd on the Law of Contract in New Zealand* (3rd ed, LexisNexis, Wellington, 2007) at [11.2.1].

269 See, for example, misleading representations as to a "rural setting", "rich environment… characterised by wetlands, streams and woods" *Draper v Pegasus Town Ltd* (2010) 12 TCLR 645 (HC) (upheld on appeal: *Pegasus Town Ltd v Draper* [2011] NZCA 140, (2011) 13 TCLR 144).

270 See discussion above at [**73**] – [**82**].

New Zealand law" or a "best global transparent exchange platform". These words are included in the Representations as *reasons why* the exchange is purportedly safe and secure: they support, and do not detract from, Cryptopia's Representations that users place on the Cryptopia exchange are safe and secure.

213 Cryptopia always understood that its users would be very interested in its approach to cybersecurity matters. For example, when Cryptopia introduced its revised terms and conditions in August 2018, it explained those new terms to its account holders as follows:[271]

> We take your security and personal information very seriously and these revised Terms and Conditions more clearly outline our policies and obligations to you.

214 Finally, the Liquidators have suggested that no reasonable reader would understand the Representations as a *guarantee* that coins traded on the Cryptopia exchange are free from the risk of a successful cyber-attack.

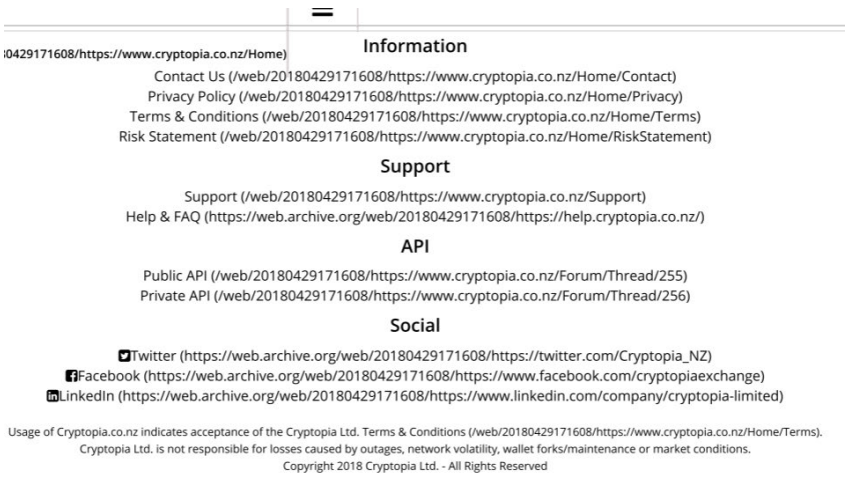
215 That is a straw man. GNY has never suggested that the Representations operated to provide users with a *guarantee* against cyberattacks. The Representations are not a promise that Cryptopia will never face a cyberattack, nor about the nature of what any such attack might involve. The Representations are about Cryptopia's approach to this type of known threat. They must be understood from the perspective of what Cryptopia itself can control, being is its own preparedness.

216 GNY considers that any reasonable reader of the Representations would understand them to mean that, Cryptopia took reasonable, or appropriate cyber-security measures to keep coins "safe" and "secure" – as you would expect of a "regulated", "ethically-run", "trusted" and "best global transparent" exchange platform. The Representations are a statement about the nature and quality of the cybersecurity measures adopted by the Cryptopia exchange, rather than an absolute guarantee against cyberattacks occurring.

---

[271] Ruscoe I, 31 July 2025, DIR1-99 – 100; [**201.0023**] at [**302.0606**] to [**302.0607**]. This email was itself arguably misleading: the changes to Cryptopia's terms were nothing to do with security and personal information.

217 Cryptopia's Risk Statement does not relevantly qualify the Representations once the nature of the Representations is properly understood[272] - even assuming that a separate document, accessible only by small font link on the website[273], which does not identify the document as commenting on cybersecurity matters, is relevant to this issue - which is not self-evident. Here is a blown-up version of the website link to the Risk Statement. This link does not give the reader any indication that clicking through this link might contain further important information about cybersecurity matters:[274]



218 The Liquidators' suggestion that "one would expect the typical consumer taking reasonable care of their own interests to have read and considered it" is not a reasonable suggestion,[275] and it is one contradicted by numerous authorities considering fine print / legalese qualifiers in a misrepresentation content – even when those exclusions are contained in the same document at the misrepresentation itself, which is not the case here.[276]

219 But, in any event, all the Risk Statement does is generically point out the risk of a hack by an external party.[277] It does not (and would be ineffective to) dissolve Cryptopia's advertised claim to

---

272 See Ruscoe I, 31 July 2025, DIR1-104 – 107; [**201.0023**] at [**301.0413**] to [**301.0416**], which suggests that Cryptopia created a draft Disclosure Statement around April 2018 because the FMA was concerned that it did not have one. Note that, by this stage, [redacted] GNY Cryptopia account was already active.

273 Or click through within Terms and Conditions which account holders were not actually required to read.

274 Ruscoe I, 31 July 2025, DIR1-110; [**201.0023**] at [**301.0427**].

275 Liquidators' Submissions, [8.103].

276 See, for example, discussion of express disclaimers in a summary judgment context, in *Pegasus Town Ltd v Draper* [2011] NZCA 140, (2011) 13 TCLR 144.

277 Ruscoe I, 31 July 2025, DIR1-104; [**201.0023**] at [**301.0413**].

have taken reasonable measures to protect itself and its users against a cyberattack.

220 Assessed more closely, the Risk Statement does not actually qualify the Representations – which are about the state of Cryptopia's security – at all, as it makes no comment on this topic.[278] It does not disclose to users of the platform that Cryptopia's platform had failed basic penetration testing on several occasions, and was subject to a numerous known critical vulnerabilities that an adequately protected cyber-exchange would have taken steps to address. These are the specific (and known) risks that Cryptopia did not include in its Risk Statement to platform users, and which directly contradict the natural meaning of the Representations. The omission of these key facts from the Risk Statement or the Representations themselves reinforces the misleading impression Cryptopia provided to users of its platform about the state of its cybersecurity.

221 Taken together, the Risk Statement and the Representations reinforce the impression that the Cryptopia has taken reasonable steps to protect the exchange and coins on the exchange from a known risk of cyberattacks. The Risk Statement identifies a generic threat, and the Representations give specific comfort to account holders that Cryptopia has taken steps to ensure its platform is "safe" and "secure" from that threat.

222 If anything, the distinction between generic risks from external attackers and the specific commitments in Representations regarding the state of the Cryptopia platform is reinforced by the *specific commitment* in the Risk Statement that Cryptopia will make reasonable efforts to disclose to account holders any technical weaknesses or system failures in the Platform. This is a commitment it did not honour with respect of the numerous technical weaknesses in its platform which it was told about repeatedly by Pulse, nor with respect to the system failures demonstrated by outcome of Pulse's penetration tests:[279]

---

278 c.f. the Liquidators' incorrect claim that the Risk Statement contains "extensive qualifications" at [8.168(c)].

279 Brocket I, 27 November 2019, at TJSB1-9 – 19; [**401.0194**] at [**401.0209**] - [**401.0219**].

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.

223 There is no material anywhere to suggest that Cryptopia made "reasonable efforts" to disclose to users the technical weaknesses it knew existed on its platform.

The Representations were misleading and deceptive

224 The Representations were misleading and deceptive in terms of ss 9, 11 & 13 of the FTA.

225 The reasons why are explained in section 5. Those submissions also address the Liquidators' contrary position as set out in their submissions.

226 Coins on the Cryptopia exchange were neither safe nor secure. Cryptopia's cybersecurity posture was significantly below the standard expected of a cryptocurrency exchange, and it was actually highly vulnerable to cyberattack. Far from being under lock and key, coins in the exchange were readily accessible to hackers: Mr Dicks' evidence confirms that Cryptopia's wallet environment was highly vulnerable to fast and easy access by hackers in the event of a malicious attack.[280]

GNY's Reliance

227 The Liquidators assert that there is no evidence that GNY was induced to list its LML token with Cryptopia by the Representations.[281] That seems a surprising commercial proposition. Anyone looking to launch their new product on a crypto-exchange would naturally be interested in security measures. The proposition is also incorrect when tested against the facts.

228 [redacted] evidence is clear that GNY was concerned to locate and trade on a safe and secure exchange, the Representations were important to its decision to list on the Cryptopia platform, and it would not have listed LML on the platform if it had known that the

---

280 Dicks I, 18 December 2025, as summarised at [12]; [**201.0154**] at [**201.0157**] to [**201.0158**].

281 Liquidators' Submissions, [8.143].

Representations were untrue.[282] There is nothing ambiguous about [redacted] evidence on this point:[283]

> A secure, safe and well-regulated exchange was important to GNY (and consistent with our business model). We would never have listed our first token on the exchange had Cryptopia not assured us that the exchange was safe and secure. Keeping our tokens safe and secure was essential to the success of the token, and so a critical factor for us in deciding where to List.

229 The Liquidators suggest this explanation is ex post-facto and "thin".[284]

230 That is a regrettable, and unfair, position to take. It again illustrates the attitude of almost blanket opposition adopted by the Liquidators. It's not clear what contemporaneous evidence of reliance on the Representations the Liquidators consider would be reasonably expected to exist: it usually the case in misrepresentation claims that actual reliance is inference from the context as a whole rather than specifically documented stipulations of reliance at the time the Representation was made.[285] If anything, it would be highly unusual to document reliance on representations contemporaneously: at the time, there would be no reason to doubt the accuracy or the representation, nor any reason to expect to need to prove reliance on a specific representation. The significance of such matters only become apparent after the fact, when it emerges that a representation was misleading. This is why, as the Supreme Court acknowledges, reliance on a representation is ordinarily inferred from circumstance.

231 GNY has always conducted itself on the basis it was misled by the Representations – including in the immediate aftermath of the Hack and prior to Cryptopia's liquidation. As [redacted] explains, GNY worked hard to engage with Cryptopia after the Hack to seek its assistance – but when Cryptopia failed to assist GNY, GNY engaged legal counsel in New Zealand and issued a proceeding against Cryptopia in the Christchurch High Court, alleging misleading and deceptive conduct in breach of the FTA on the basis of the

---

282 [redacted] 19 December 2025, at [62]–[64]; [**201.0141**] at [**201.0153**].
283 [redacted] 19 December 2025, at [64]; [**201.0141**] at [**201.0153**].
284 Liquidators' Submissions, [8.144].
285 The Supreme Court acknowledged reliance is usually a matter of inference from the evidence as a whole in *Red Eagle Corp Ltd v Ellis* [2010] NZSC 20, [2010] 2 NLZR 492 at [29].

Representations, and served that claim on Cryptopia.[286] This proceeding precipitated Cryptopia's appointment of liquidators. Since that time, GNY has spent considerable time and money pursuing these allegations, and there is no reasonable (or factual basis) to suggest that its reliance on the Representations is not genuine, or that [redacted] should be disbelieved.

232 GNY's reliance on Cryptopia's Representations to inform it of whether Cryptopia adopted reasonable, industry-appropriate, cybersecurity measures was perfectly reasonable in context:

232.1 All traders on Cryptopia's platform – but particularly those listing new tokens – would naturally, and reasonably, be interested in Cryptopia's assurances about the safety and security of the platform. The consequences of a hack can be (and in this case was) devasting for a new coin listing.[287]

232.2 Traders on Cryptopia's platform had no way of independently interrogating Cryptopia's cybersecurity posture, notwithstanding the importance of this issue to any successful cryptocurrency exchange.

232.3 Cryptopia's own statements, on its website, were, in all the circumstances, the best available source of information to traders about the state of Cryptopia's cyber-security.

233 Finally:

233.1 The Liquidators suggest that "there were plenty of reasons why GNY would have wanted to list LML on the Cryptopia that have nothing to do with security".[288] This is irrelevant. Of course there were various reasons why GNY listed LML on Cryptopia in addition to Cryptopia's assurances that its platform and coins stored on it were safe and secure.[289] All would be fatally undermined if Cryptopia could not provide a secure platform. It is, in any event, well-established that "the

---

286 [redacted] 30 March 2025, at [26]; [**201.0001**] at [**201.0006**]. The Liquidators were appointed weeks after GNY issued its claim.

287 See [redacted] description of the devastating effects of the Hack on GNY: [redacted] 19 December 2025, at [6]–[32]; [**201.0141**] at [**201.0142**] to [**201.0147**].

288 Liquidators' Submissions, [8.145].

289 [redacted] iscusses GNY's commercial drivers in his evidence: [redacted] 19 December 2025, at [62]–[64]; [**201.0141**] at [**201.0153**].

representation need not be the sole inducement. It is sufficient so long as it plays some part even if only a minor part in contributing to the formation of the contract".[290] It is equally well established that reliance can be based on generalised expectations rather than a specific explanation for why a person purchased the goods and services in question.[291]

233.2 The Liquidators' submissions about on the absence of evidence regarding GNY's listing with Bitbay is misplaced. GNY is not bringing a claim against Bitbay on any matter, and evidence about its listing on that platform is not necessary to prove (nor even logically connected to) its reliance on Cryptopia's Representations. There is certainly no basis for the Liquidators' conclusion that "[t]he pattern of conduct suggests GNY's primary concern was to list LML on as may exchanges as possible to maximise exposure and trading volume, rather than to select exchanges on the basis of their security credentials".[292] This is an entirely speculative submission, and contradicted by all the available evidence, including the fact that GNY only ever listed LML on two exchanges, Cryptopia and Bitbay.

Causation of GNY's loss

234 Moreover, having induced GNY to list the LML token on the Cryptopia platform through the Representations, the inaccuracy of the Representations is directly causative of GNY's loss.

235 This is because, as Mr Dick's explains,[293] Cryptopia's specifically identified cybersecurity failings were directly exploited by the hackers to ensure the Hack was successful.

236 There is no basis on which it could reasonably be concluded that the Hack was an indomitable or invulnerable event. Rather, the evidence suggests that Cryptopia had abysmally weak security

---

290 *Gould v Vaggelas* (1985) 157 CLR 215 at 236, as cited by Debbie Wilson "Time Limitation and Causation Requirements" in *The Fair Trading Act Handbook (2018)* (LexisNexis, Wellington, 2018) at [16.76]. See also *Ackers v Austcorp International Ltd* [2009] FCA 432 at [177].

291 *Minister of Education v James Hardie NZ and Carter Holt Harvey Ltd* [2014] NZHC 2432 at [99].

292 Liquidators' Submissions, [8.149].

293 And is more fully addressed at [**100**] –[**117**].

features.[294] The evidence further suggests that those features were easily breached using a common methodology (a phishing email), and that attack resulted in Hackers obtaining easy and fast access to *all* of Cryptopia's network, including its wallet environments in old and new servers, easily and for days.[295]

237 Put another way, the evidence suggests that if the Representations had been true – and Cryptopia *had* adopted adequate cyber-security features – the Hack may well have been prevented, or stopped, before any coins were taken.[296]

238 The fact that the hackers are third parties is irrelevant, much less a "a break in the chain of causation".[297] A Court will ordinarily find causation proved in the event that the misleading conduct was *an* operating cause of loss, even if there are other effective causes of loss.[298] And, as was addressed earlier in these submissions, the Liquidators' claims that the Hack was "exceptional" or virtually unstoppable, is both irreconcilable with the expert evidence, and based on unsound reasoning.[299]

239 Finally, the evidence establishes that Cryptopia was in a position to secure the stolen LML post-Hack, but did not. Bitbay was unable to permanently freeze the stolen LML because of Cryptopia's inaction - and not for any reason independent of Cryptopia's own conduct.[300]

Cryptopia's FMCA breach

240 The FMCA and FTA concurrently regulate financial services.

---

294 Dicks I, 18 December 2025, at [55]; [**201.0154**] at [**201.0173**] to [**201.0174**], for example only.

295 Dicks I, 18 December 2025, at [76]–[85]; [**201.0154**] at [**201.0180**] to [**201.0182**].

296 See above at [**100**]–[**117**]. Dicks I, 18 December 2025, [76]–[85]; [**201.0154**] at [**201.0180**] to [**201.0182**], and see the summary of Mr Dicks' conclusion on this issue at [12.8]; [**201.0154**] at [**201.0158**]–[**201.0159**].

297 Liquidators' Submissions, [8.153]

298 See, for example, *Dalecoast Pty Ltd v Guardian International Pty Ltd* [2003] WASCA 142 at [55], explaining that the conduct in question only need be "a" cause of loss, not "the" cause of loss.

299 See above at [**100**]–[**117**].

300 See above at [**179**]–[**189**]. [redacted] 19 December 2025, at [5]–[32]; [**201.0141**] at [**201.0142**] to [**201.0147**]. This allegation by the Liquidators is also obviously irrelevant to the fiduciary cause of action, given the "narrow escape route" from paying equitable damages arising from breach to which fiduciaries are subject.

241 The FMCA fair dealing provisions also, in ss 19, 21, and 22, prohibit misleading and deceptive conduct generally and in relation to financial services.

242 The Representations breach each of these provisions, for substantially the same reasons as they breach the FTA.

243 The criteria in s 24 (to which the Court must have regard when ascertaining breach) reinforce the earlier analysis: the nature of the services means that cybersecurity is a critical matter for traders (s 24(1)(a)), the representation concerns quality rather than quantity (s 24(1)(b)), the information the representation concerns (protective measures) is held by Cryptopia and is not otherwise accessible to traders (s 24(1)(c)), the source of the information was Cryptopia (s 24(1)(d)), and the effect of the Representations on GNY was to induce it to list LML on the Cryptopia platform (s 24(1)(f)).

Cryptopia's CGA breach

244 GNY alleges that Cryptopia provided its cryptocurrency exchange platform in breach of s 28 of the Consumer Guarantees Act 1993 (**CGA**), a breach of the guarantee of reasonable skill and care.

GNY was a CGA consumer of a CGA service

245 The Liquidators have suggested that GNY is a not a "consumer" for the purposes of the CGA. The Liquidators rely on whether GNY was purchasing services from Cryptopia as a consumer *itself*. But the focus of the test is the type of service, and whether it is typically for personal use.[301]

246 A consumer is defined as a person who "acquires from a supplier… services of a kind ordinarily acquired for personal, domestic or household use or consumption".[302] Goods "ordinarily" for personal use do not have to be acquired for personal use by all, or even the majority, of the users.[303]

247 Once the initial threshold in the definition of consumer is passed, as it is in this case, there are only two potentially relevant qualifiers on who may be a "consumer" for the purposes of consuming services under the CGA. Neither of the potentially applicable qualifiers are relevant to GNY:[304]

247.1 The first exception applies to a person who receives services for "resupplying them in trade". This is not what GNY did. Rather, it used the platform to facilitate trading in tokens – with other traders on the platform.

247.2 The second exception would apply if GNY consumed the services "in the course of a process of production or manufacture". Again, this is not how GNY used the platform. The Cryptopia exchange provided a platform for trading GNY's tokens, it was not subsumed into them.

---

301 Liquidators' Submissions, [8.182]–[8.185].
302 Consumer Guarantees Act 1993, s 2(a).
303 See, for example, *Nesbit v Porter* [2000] 2 NZLR 465 (CA) per [29], where 20% of users of the product in question were said to be domestic
304 Consumer Guarantees Act 1993, s 2(b).

Cryptopia's CGA breach

248 GNY claims that the services supplied by Cryptopia to it were not supplied to a reasonable standard of skill and care. The reasons for this claim are essentially the same as those advanced with respect to Cryptopia's breach of its fiduciary duties and with respect to the misleading nature of the Representations.[305]

Cryptopia's breach of contract

Cryptopia's obligation

249 In addition to the fiduciary and statutory claims described above, Cryptopia has breached its contractual commitments to GNY as a result of its failure to properly manage and provide services with reasonable care on its platform.

250 The relevant clause in Cryptopia's terms and conditions is as follows:[306]

> 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.

251 The Liquidators suggest that this clause provides a duty limited to "take reasonable care to prevent disruptions and errors on the Platform, namely in relation to maintenance".[307]

252 This is not what clause 8(a) says. It says that Cryptopia will "take reasonable care in operating our Platform, so as to limit disruptions to the Platform, User Accounts and our Services". That promise is unqualified.

253 Neither disruptions nor Business Disruptions is defined elsewhere in the Terms & Conditions. The provision of security measures is within the scope of Cryptopia's operation of the Platform on any plain understanding of the word "operation". Equally plainly, a hack

---

305 See Section 5 above, which provides an overview of Cryptopia's defective cybersecurity posture, underpinning this claim.

306 Brocket I, 27 November 2019, at TJSB1-9 – 19; [**401.0194**] at [**401.0212**] - [**401.0219**].

307 Liquidators' Submissions, [8.197].

– especially a catastrophic one – is a disruption to the Platform, the User Accounts, and Services. This is because the Terms define Services as services which "allow you to… buy, sell and exchange supported Coins through the Platform… and store supported Coins in our hosted Wallets". The Hack plainly disrupted the Services.

254 The proposition that the clause is limited to maintenance cannot be sustained. Users accept that accounts "may also be inaccessible from time to time while undergoing maintenance or upgrade work". This is not the full scope of the clause as a whole, or the reference to "also" would be redundant. Rather, the full scope of the clause is that Cryptopia will take reasonable care when operating the Platform so as to limit disruptions – and, subject to that commitment, users must accept that the Platform will not be error-free, for various reasons, which may include maintenance work.

255 The Liquidators' have also suggested that GNY has presented no context for its preferred interpretation.[308] However, relevant context includes the Representations Cryptopia made to its account holders on its website - and the fact that cybersecurity risks were well known for Platform disruptions in the industry.[309] Even the Risk Statement, which is cross-referenced and incorporated into the Terms and Conditions, reinforces the link between hacks, technical failures and maintenance: all three are dealt with under the same heading as "systems risks" between clauses 11 and 16 of that statement.[310]

256 Moreover, the Risk Statement makes a specific commitment in connection with "technical weakness", or "system failure" or "hack" (all in the same clause):[311]

> 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.

308 Liquidators' Submissions, [8.198].
309 See the Representations made by Cryptopia at [**201**] – [**223**].
310 Ruscoe I, 31 July 2025, DIR1-105 – 106; [**201.0023**] at [**301.0414**] to [**301.0415**].
311 Ruscoe I, 31 July 2025, DIR1-106; [**201.0023**] at [**301.0415**].

257 Cryptopia did not advise any of its accountholders that the Platform was subject to "technical weakness" or "system failure" – notwithstanding that it obviously was, as demonstrated to and known to Cryptopia as a result of the various Pulse reports and internal records demonstrating it knew its platform was unacceptably vulnerable.[312]

Breach

258 Cryptopia did not use reasonable care in operating the platform.

259 The reasons for this claim are essentially the same as those advanced with respect to Cryptopia's breach of its fiduciary duties and with respect to the misleading nature of the Representations and with respect to breach of the CGA: Cryptopia failed to provide an adequate (or reasonable) level of cybersecurity for its platform, as would be expected for any competent operator of a crypto-currency exchange.[313]

Causation

260 Cryptopia's breach of contract caused GNY's loss for essentially the same reasons as are set out at [**227**] – [**239**] above.

Cryptopia's negligence

Absence of reasonable care

261 There's no question that accountholders like GNY are proximate to Cryptopia in the manner ordinarily required for a duty of care to arise.

262 The Liquidators have suggested, however, that Cryptopia may have discharged its duty of reasonable care, as "it is not clear what more the reasonable person could have or would have done in the circumstances" regarding Cryptopia's known cybersecurity vulnerabilities.[314]

263 This submission is difficult to credit, but appears to be based on the incorrect proposition that Cryptopia implemented "at least 50% of those recommendations" from its cyber-security experts.[315] That

---

312 See discussion of Cryptopia's knowledge and failure to address its cybersecurity vulnerabilities at above at [**143**] – [**178**].

313 See discussion of Cryptopia's inadequate security measures at Section 5.

314 Liquidators' Submissions, [9.14].

315 Liquidators' Submissions, [9.13(b)].

statement appears to be based on a misread of a specific document,[316] and is not an accurate summary of the steps Cryptopia took in response to the warnings it received about its unacceptably vulnerable cybersecurity state.[317]

Causation

264 Cryptopia's breach of duty caused GNY's loss, for essentially the same reasons as are set out at [**227**] – [**239**] above.

GNY claims: relief

265 The basis of GNY's claims to relief are:

265.1 Equitable damages, for Cryptopia's breach of its fiduciary duty of honesty and good faith.

265.2 Compensatory damages, under s 43(3)(f) of the FTA, which permits the order of compensation for any person who has suffered loss or damage by the conduct of another in breach of the applicable FTA provisions.[318]

265.3 Compensatory damages, under ss 494(1) & 495(1) of the FMCA, which permits a wide discretion to the Court to order compensatory damages on a similar basis to that provided for in the FTA, if the Court considers it "just" to make such an order.

265.4 Compensatory damages, under s 32(c), damages for loss resulting from Cryptopia's failure to comply with the CGA, for

---

316 Cryptopia's October 2018 "virtual CISO" report notes that benchmarking demonstrated Cryptopia had partially adopted 50% of the "essential eight" fundamental security measures, which is a different observation from whether Cryptopia had implemented any of Pulses' recommendations. See Ruscoe I, 31 July 2025, DIR1-345; [**201.0023**] at [**302.0729**]. Relevantly, these "fundamental security measures" are basic must-haves which Cryptopia did not yet have - let alone implemented the actual recommendations it had received from its advisors. Moreover, even this document, read in full, does not support the submission that it is hard to see what more Cryptopia could have done on cybersecurity: the overall tenor of the document is that Cryptopia had deprioritised required steps, remained highly vulnerable to attack, and was far below any acceptable standard of security for a cryptocurrency exchange.

317 These matters, and Cryptopia's failure to take required steps, are more fully addressed at [**143**] – [**178**].

318 In this case, the step GNY took in reliance on the Representations was to list LML on the platform: its losses flow from that event, being the theft of LML, and consequent effects on LML's market capitalisation.

losses that were reasonably foreseeable as liable to arise from the failure.

266 While each of these heads of loss have different purposes, with the exception of equitable damages, they have the same conceptual underpinning: compensation for loss.

267 Equitable damages reflect the fiduciary nature of the underlying duty, and as such it may be possible to obtain non-compensatory equitable damages. However, in this case, the focus of GNY's equitable damages claim is loss that it suffered as a result of Cryptopia's breach of its obligations (rather than non-compensatory remedies such as disgorgement). As a result, the measure of loss should be the same across each of the causes of action.[319]

268 Before turning to that loss (section 9), these submissions first address:

268.1 whether GNY or other Hack victims are precluded from claiming any or most of their loss by virtue of Cryptopia's purported exclusion clauses (section 7); and

268.2 whether GNY and other Hack victim losses should be assessed in BTC, rather than NZD (section 8).

[319] As it was in, for example, *Stephens v Premium Real Estate* [2009] NZSC 15, [2009] 2 NZLR 384 at [111] per Tipping J (and see this judgment generally treating equitable compensation *for loss*, and damages for breach of the FTA, on the same basis, with distinctions arising in connection with non-compensatory claims for disgorgement, and refund of commission.)

SECTION 7: NO EXCLUSION OF CRYPTOPIA'S LIABILITY

Overview

269 The Liquidators allege that Cryptopia fully excluded all liability to GNY (other than on claims where the law explicitly precludes such contracting out).[320] The basis for this position is clause 12.1 of the Terms and Conditions (the **Exclusions**), which Cryptopia purportedly incorporated into its standard terms in August 2018.

270 Clause 12.1 reads as follows:[321]

> 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:
>
> *[list of 12 non-exhaustive types of losses or Cryptopia failures, including any breach of the Terms and Conditions, any interruptions to the Platform, unauthorised access to customer accounts etc]*
>
> 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.

271 Clause 12.1 presents a notably extreme exclusion clause: on its face, it is a purported total exclusion of Cryptopia's liability to account holders on any basis whatsoever (save that it purports to preserve such FTA and CGA rights a User may have, subject to an aggregate cap of $5,000).[322]

---

320 Ruscoe I, 31 July 2025, at [24(b)]; [**201.0023**] at [**201.0032**].
321 Brocket I, 27 November 2019, TJSB1-14; [**401.0194**] at [**401.0214**].
322 The Liquidators' Submissions portray the construction of these clauses as the primary issue: see [8.49]–[8.61]. GNY's position is that the clauses are onerous and unenforceable, including on the expansive interpretation supported by the Liquidators. Therefore, the correct analytical approach is to consider (a) are the clauses onerous and (b) were they properly incorporated into the contract with sufficient notice.

272 If the Liquidators were correct on the effect of the Exclusions:

272.1 Cryptopia would have no contractual liability to any account holder for breach of contract, nor any tortious liability for breach of a duty of care. Cryptopia's performance of its obligations would essentially become optional. However poorly it conducted itself, account holders would have no common law recourse;

272.2 GNY's claims against Cryptopia under the CGA or FTA would be capped at $5,000; but

272.3 GNY's fiduciary duty and FMCA claims would be unaffected because, as the Liquidators accept, they cannot be contracted out of.[323]

273 The Exclusions did not, however, form part of the contract between GNY and Cryptopia, do not bind GNY, and are in any event unenforceable (or simply not applicable) in connection with a range of GNY's claims.

Cryptopia's purported incorporation of the Exclusions

274 When assessing the enforceability of exclusion clauses, it is important to understand how those clauses were purportedly incorporated into the parties' contract as a matter of fact.

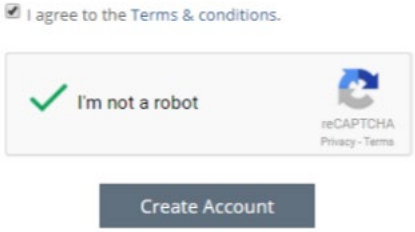
275 This is because, at a high level (and as is expanded on in more detail below), exclusions that reflect the expressly negotiated position of commercial parties are much more likely to be properly incorporated in the parties' bargain and enforceable than standard form exclusions which are imposed by one party in a context where negotiation is not realistically possible. Cryptopia's attempt to incorporate the Exclusions into its Terms and Conditions sits very much at one end of that spectrum.

Cryptopia account opening process

276 Cryptopia's terms and conditions were addressed only once in the Cryptopia account opening process. To set up an account, users were required to provide an email and password. On provision of

[323] Ruscoe I, 31 July 2025, at [24(b)]; [**201.0023**] at [**201.0032**].

those details, the user was taken to click on an "I agree to the terms & conditions" box, where the terms were hyperlinked in small text. The below screenshot, taken from Cryptopia's FAQs page, illustrates this process.[324]



277 An email verification process followed this. Users had to confirm their email and then input the code provided to that email address to verify their account.

278 The "clickwrap"[325] box above is the sole instance where Cryptopia's account holders are alerted to the terms during the account opening process. The terms are not mentioned in the verification emails.[326] Users were not required to click on that hyperlink to open the terms before clicking the box. They were not required to read the terms, nor was there any requirement for account holders to scroll the terms before clicking to confirm agreement.

279 Through this process, the Exclusions in the Terms and Conditions (and a similarly expansive exclusion in the earlier terms and conditions in effect before August 2018) were evidently not drawn to the attention of account holders at the time they opened their accounts.

280 Nor was Cryptopia's Risk Statement referred to anywhere in the account opening process. An account holder would not necessarily know it existed unless they:

---

324 Brocket, 27 November 2019, TJSB1-39 – 42; [**401.0194**] at [**401.0239**] - [**401.0242**].
325 See the "clickwrap" case specific discussion below at [**301**] – [**311**].
326 To the extent shown in the Brocket affidavit.

280.1 accessed it on Cryptopia's website separately (where it could be found via a small print link alongside various other legal documents);[327] or

280.2 if they opened Cryptopia's Terms and Conditions, read them, identified that they included a reference to a Risk Statement, and clicked through to the Risk Statement from clause 7.1(a)(iv) on page 10.[328]

281 GNY in any event does not consider that the Risk Statement has any particular legal relevance to whether the Exclusions were effectively incorporated into Cryptopia's Terms & Conditions.

Pre-August 2018 accounts ([redacted]

282 Cryptopia's terms and conditions prior to August 2018 allowed it to make changes to the terms unilaterally, with continued use of the site deemed acceptance of any changes.[329]

283 In August 2018, Cryptopia amended its standard terms to incorporate the Exclusions.[330] The [redacted] account was in existence on the date on which Cryptopia purported to incorporate the Exclusions into its Terms and Conditions. [redacted] experience with that account is indicative of other account holders at that time.

284 Cryptopia advised existing account holders of changes to the Terms and Conditions by email expressed in the following terms:[331]

> 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*.

---

327 Ruscoe I, 31 July 2025, DIR1-110; [**201.0023**] at [**301.0427**].
328 Ruscoe I, 31 July 2025, DIR1-86; [**201.0023**] at [**302.0583**].
329 Ruscoe I, 31 July 2025, DIR1-96; [**201.0023**] at [**301.0002**]. These submissions capitalise "Terms and Conditions" when referring to the post-August 2018 Terms and Conditions only.
330 Brocket I, 27 November 2019, TJSB1-39 – 42; [**401.0194**] at [**401.0239**] - [**401.0242**].
331 Ruscoe I, 31 July 2025, DIR1-99 – 100; [**201.0023**] at [**302.0606**] to [**302.0607**].

> 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.
>
> (emphasis added)

285 While the email did recommend account holders read the revised Terms and Conditions, it did not require users to take that step. Nor did it draw attention to the purported Exclusions.

286 In fact, the email advised users that the purpose of the update to the Terms and Conditions was to "maintain our commitment to operate as a regulated cryptocurrency exchange" — suggesting that changes to the Terms and Conditions reflected regulatory requirements for the benefit of users. Later in the email, Cryptopia strongly implies that the changes to the Terms and Conditions concern security and personal information, and simply "more clearly outline our policies and obligations to you".[332]

287 Neither of these comments amounts to an accurate description of the purpose and effect of the revised Terms and Conditions. Readers of this email would have no reason to expect that the revised Terms and Conditions would, on their face, render Cryptopia's performance of its contractual obligations effectively optional. Rather, the email suggested term changes were for the benefit of Users, rather than for the benefit of Cryptopia.

Post-August 2018 accounts ([redacted]

288 The account associated with [redacted] was not created at the time that Cryptopia advised account holders of the changes to the Terms and Conditions. His only engagement with the Terms and Conditions was via the perfunctory "clickwrap" box tick required as part of the Cryptopia account opening process.

GNY's engagement with Cryptopia on listing LML

289 The Terms and Conditions were not drawn to GNY's attention in the course of its engagement with Cryptopia on listing LML on the exchange.[333] Relevantly, none of the Listing Form, Listing Contract,

---

332 Ruscoe I, 31 July 2025, at DIR1-100; [**201.0023**] at [**302.0606**].
333 The parties' exchanges on the listing of LML are summarised at paragraph [**56**] above.

nor the parties' email exchanges mention the Terms and Conditions, let alone the Exclusions.

The Trust Decision

290 Before turning to the applicable legal principles, the Liquidators have suggested that the Trust Decision may be "binding" on this Court in respect of the Terms and Conditions, including the enforceability of the Exclusions.[334]

291 That suggestion may be dealt with briefly. As the Liquidators appropriately acknowledge, the Trust Decision "did not expressly consider" the Exclusions,[335] and was "primarily for the purpose of determining whether the cryptocurrencies were held on trust".[336]

292 The Trust Decision did not expressly consider the Exclusions because no issue before the Court required it to do so. No submissions were addressed to the question of the Exclusions. The law concerning the incorporation of Exclusion clauses into contracts was not cited to the Court by counsel, or by the Court in its decision. The question of whether cryptocurrencies were held on trust engages quite different legal considerations to whether Exclusion clauses are effectively incorporated into the parties' contract and are therefore enforceable. Generalised comments made by the Court about the Terms and Conditions overall cannot be understood as creating a "binding" ratio on a different legal question not actually before the Court at the time (even before considering that GNY was not a party to the Trust Decision).

Legal framework

Onerous clauses & "sufficient attention" requirement

293 The Liquidators say that the starting point for legal analysis is "contractual freedom" and the clarity of the clauses in question.[337]

294 But onerous clauses such as exclusion clauses are not ordinary contractual clauses. Where, as here, they purport to completely exclude liability for contractual breach, such clauses are not, on their face, consistent with contractual freedom: rather, they operate

---

334 Liquidators' Submissions, [6.5].
335 *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728, [2020] 2 NZLR 809; [**401.0365**]. Liquidators' Submissions, [6.6].
336 Liquidators' Submissions, [6.6].
337 Liquidators' Submissions, [8.49(a)].

as a challenge to the very concept of enforceable contractual obligations. This is particularly the case where those terms are purportedly incorporated by non-negotiable standard form (as is the case here) or where the terms are purportedly incorporated by clicking a button, rather than signing in a conventional manner (as is also the case here).

295 Against that background, the law of exclusion clauses has developed over the last 50 years in parallel to the ordinary requirements of contract formation in order to "mitigate the rigours of such a regime".[338] That law blunts reliance on concepts of contractual freedom where onerous contractual terms are obfuscated and unfair, and the parties' bargaining position is unequal.

296 The decision in *Interfoto Picture Library*[339] is illustrative of the orthodox approach to onerous clauses, including exclusion clauses. The Court held a late fee clause, imposing a charge of £5 a day, was so onerous as to require being drawn to the specific attention of the contracting party. Because that had not occurred, the clause was unenforceable.[340] Dillon LJ referred to obiter by Denning LJ in *J Spurling Ltd v Bradshaw*:[341]

> Some clauses which I have seen would need to be printed in red ink on the face of the document with a red hand pointing to it before the notice could be held to be sufficient.

297 Generally, "the more outlandish the clause, the greater the notice which the other party, if he is to be bound, must in all fairness be given".[342] In *Livingstone v Roskilly,* the Court held an unduly onerous clause was one that is:[343]

297.1 particularly onerous or unusual; and / or

297.2 abrogates ordinary common law rights.

---

338 *Livingstone v Roskilly* HC Auckland M568/91, 2 March 1992 at 18. See also *Parker-Grennan v Camelot UK Lotteries Ltd* [2024] EWCA Civ 185 at [1]–[8].
339 *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd*. [1989] QB 433 (CA).
340 *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd*. [1989] WB 433 (CA) at 352 and 357–358.
341 *J Spurling Ltd v Bradshaw* [1956] 1 WLR 461 (CA) at 466.
342 *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd*. [1989] QB 433 (CA) at 355.
343 *Livingstone v Roskilly* [1992] 3 NZLR 230 (HC).

298 Therefore, the key starting questions are whether the Exclusions are onerous, and whether the Exclusions were specifically brought to the attention of GNY (or any other Cryptopia account holder). If an onerous clause is fairly and reasonably drawn to the attention of a contracting party, and then the contract is signed by that party, the party will usually be bound by those terms (whether or not the contract was in fact read by the party).[344] However, the critical precondition is that the onerous clause is fairly and reasonably drawn to the party's attention.

299 Whether "sufficient notice" has been provided is a question of fact in all the circumstances of the particular case. While the Liquidators have suggested in their submissions that the law may not impose a less stringent "sufficient notice" requirement for onerous clauses on commercially astute parties,[345] this suggestion is incorrect.[346] The courts have resisted confining the principle to particular categories of cases, preferring a case-by-case analysis.[347]

300 In addition, even where exclusion clauses are incorporated into a contract because the sufficient notice requirement is met, those clauses are typically construed narrowly. Generally:

300.1 doubt as to the meaning and scope of exclusion clauses will be resolved against the party who relies on them (the contra proferentem rule);[348]

---

344 *Toll (FGCT) Pty Limited v Alphapharm Pty Ltd* [2004] HCA 52 at 185. See also *Ravensdown Fertilizer Co-op Ltd v Eveleigh* [2012] NZHC 660 at [38].

345 Liquidators' Submissions, [8.49(c)]. This submission is based on an apparently obiter comment in *Jardboranir hf t/a Iceland Drilling v Summit Hydraulic Solutions Ltd* [2016] NZHC 490 at [40] per Brewer J to the effect that he was not aware of any case where Denning LJ's "red ink" dicta has been applied to commercially astute parties. On the facts before it, the Court found that the clauses pointed to were not actually onerous (at [41]). And in any event, those facts differ materially from the present case, involving two parties with equal negotiating power and terms actually supplied from one to the other, unlike this case. Both parties also had a record of commercial operation in New Zealand. Regardless, as is explained in these submissions, the "red ink" requirement has been applied in commercial cases, and the question of what is required to draw sufficient attention to an onerous exclusion clause is really a question of context and circumstance, of which the nature of the parties is just one.

346 See, for example, *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm).

347 *Livingstone v Roskilly* HC Auckland M568/91, 2 March 1992 at 14.

348 Matthew Barber, Stephen Todd, *Burrows, Finn and Todd on the Law of Contract in New Zealand* (LexisNexis, online ed, 2022) at 242–243.

300.2 the contra proferentem rule's application is limited where exclusion clauses were negotiated by express agreement[349] between parties of equal bargaining power;[350] and

300.3 the contra proferentem rule's most common application tends to be in the exclusion clause context; parties are presumed to not lightly give up valuable remedies in the face of breach.[351]

"Clickwrap" onerous clauses

301 The Liquidators' Submissions do not address the "clickwrap" nature of Cryptopia's purported incorporation of the Exclusions. "Clickwrap" refers to the practice of clicking "I agree" next to a tick box to signal one has agreed to the relevant terms and conditions online.

302 There is a growing body of international case law that recognises the challenges in ensuring that parties to terms and conditions agreed online properly understand those terms and conditions.[352] The Liquidators' Submissions do not consider these decisions.[353]

303 The Liquidators' reliance on obiter comment in the New Zealand decision of *Jardboranir* for the proposition that "the requirement for notice is less stringent in a commercial context" illustrates some of the differences between a typical commercial context, and an online "clickwrap" context.[354] While the terms and conditions agreed to in *Jardboranir* were standard form, they were also supplied via email, printed out, physically signed and sent back to the party proposing

---

349 *Modern Engineering (Bristol) Ltd v Gilbert-Ash (Northern) Ltd* [1974] AC 689 at 717H, cited in *Triple Point Technology v PTT* [2021] UKSC 29, [2021] 3 WLR 521 at [109].

350 *Persimmon Homes v Ove Arup* [2017] EWCA Civ 373 at [52]; see also *Pinewood Technologies Asia Pacific Ltd v Pinewood Technologies Plc* [2023] EWHC 250 at [82(d)].

351 Matthew Barber, Stephen Todd, *Burrows, Finn and Todd on the Law of Contract in New Zealand* (LexisNexis, online ed, 2022) at 242–243; *Triple Point Technology Inc v PTT Public Co Ltd* [2021] UKSC 29, [2021] 3 WLR 521 at [106].

352 See the discussion at *Parker-Grennan v Camelot UK Lotteries Ltd* [2024] EWCA Civ 185 at [1]–[8]. *Spreadex Ltd v Cochrane* [2012] EWHC 1290 (Comm) at [21]; *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm); *Nicosia v Amazon.com Inc,* No. 15-423 (2d Cir. 2016).

353 These issues don't appear to have been considered as thoroughly in New Zealand: there is some limited discussion with regard to the FTA in *Commerce Commission v viagogo AG* [2024] NZHC 713.

354 Liquidators' Submissions, [8.49(c)]; *Jardboranir hf t/a Iceland Drilling v Summit Hydraulic Solutions Ltd* [2016] NZHC 490.

those terms. Months of commercial discussion and contact preceded this event.[355]

304 Cryptopia's process for agreement to the Terms and Conditions was entirely different: a click box, to be addressed in a matter of seconds, as one (small) part of a multi-stage verification account onboarding process — with no indication given as to the nature of what terms the account holders were signing onto. The digital nature of the contract is not conducive to inferring that the recipient party has had opportunity to give proper consideration to the imposed terms.

305 GNY refers to three English decisions that consider the incorporation of terms into a contract in a digital environment.

306 In *Blu-Sky Solutions Ltd v Be Caring Ltd*, Blu-Sky, a telecoms dealer, sued Be Caring Limited (*BCL*) for £180,000 plus VAT after BCL signed an order form for 800 EE[356] mobile connections over 48 months and then cancelled before connection.[357] Blu-Sky relied on standard terms imposing an "administration charge" of £225 per connection.

307 The Court held the order form created commercial relations, but the administration fee clause was particularly onerous — and it had not been fairly and reasonably brought to BCL's attention. Blu-Sky's order form was sent via an Esign application. It referenced Blu-Sky's standard terms and conditions. There was a statement requiring the signatory to confirm they had logged onto Blu-Sky's website and read and agreed to those terms. A clickwrap box was below this statement: it could be "signed" without anyone reviewing the terms or logging onto the website.[358]

308 The terms and conditions were in "closely spaced small type" with "no separate clause headings".[359] The Judge held the administration fee clause was particularly onerous. The amount bore no relationship to true administration costs and was out of all

---

355 *Jardboranir hf t/a Iceland Drilling v Summit Hydraulic Solutions Ltd* [2016] NZHC 490 at [6]–[15].
356 An English mobile provider.
357 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm).
358 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [40]–[41].
359 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [53].

proportion to any reasonable estimate of loss resulting from cancellation.[360]

309 The Judge found the terms were not fairly and reasonably brought to BCL's attention. The order form did not explain the essential purpose of the terms; it obfuscated the nature of the contract, misleading BCL into believing it was signing an order form as a precursor to a contract rather than entering into a contract with substantial cancellation liability.[361] The terms could easily have been included with the order form or sent with a prominent heading explaining onerous provisions. The administration fee clause was buried within section 4, innocuously titled "cancellation and returns policy", which was itself buried in the middle of lengthy terms and conditions.[362]

310 *Green v Petfre (Gibraltar) Ltd (t/a Betfred)* is an example of bare clickwrap acceptance being insufficient to incorporate onerous terms. Inadequate signposting, onerous terms being buried in other materials, unhelpful presentation and a gap of 4.5 years between the clickwrap acceptance and the relevant incident all led the Court to conclude it was "quite unreasonable" to have expected Mr Green to have read and understood the clauses relied on in this context.[363]

311 In *Parker-Grennan v Camelot,* the Court upheld clickwrap acceptance. The terms were well signposted, summarised in dropdown menus, available on request in hardcopy and required agreement before players could continue when significant updates were imposed.[364] Critically, the terms Camelot relied upon were "neither onerous nor unusual" — they were game-procedure, validation and dispute-resolution provisions. The terms "merely set out what is required in order to achieve the entitlement to be paid the prize money" — they did not "impose any burden on the player".[365] The Court carefully noted that clickwrap would not be

---

360 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [109].
361 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [110].
362 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [110].
363 *Green v Petfre (Gibraltar) Ltd (t/a Betfred)* [2021] EWHC 842 (QB) at [166], [167] and [168].
364 *Parker-Grennan v Camelot UK Lotteries Ltd* [2024] EWCA Civ 185 at [42], [49] and [56].
365 *Parker-Grennan v Camelot UK Lotteries Ltd* [2024] EWCA Civ 185 at [34] and [36].

"sufficient to incorporate all the *standard* terms and conditions in every case".[366]

Exclusions not incorporated into Cryptopia's Terms and Conditions

The Exclusions are onerous

312 The Liquidators' suggestion that the Exclusions do not amount to an onerous clause as a matter of contract law is surprising.[367] On their face, the Exclusions purport to exclude all contractual, tortious, and all other liability (save for liability under the CGA or FTA), rendering Cryptopia's performance of its contractual and tortious obligations optional. They purport to permit narrow statutory liability under the CGA and FTA for some users only — but with a constrained limitation of liability at $5,000.

313 The Exclusions "hollow out" Cryptopia's contractual obligations in a manner that undermines the purpose of a binding agreement. An exclusion clause which defeats the purpose of the contract by rendering its performance optional is, as a matter of principle, so onerous that it will not be enforceable per se, irrespective of whether it has been drawn to the counter-party's attention.[368]

314 Lord Wilberforce observed that parties cannot be taken to have intended an exclusion clause to have "so wide an ambit as in effect to deprive one party's stipulations of all contractual force", since that would reduce the contract to "a mere declaration of intent".[369] His Lordship further observed that the more radical the breach said to be covered, the clearer the language required. As noted by the learned authors of *Burrows, Finn and Todd*, exclusion clauses

---

366 *Parker-Grennan v Camelot UK Lotteries Ltd* [2024] EWCA Civ 185 at [47].

367 Liquidators' Submissions, [8.63].

368 *Suisse Atlantique Société d'Armement Maritime SA v NV Rotterdamsche Kolen Centrale* [1966] 2 All ER at 92, see also *Pinewood Technologies Asia Pacific Ltd v Pinewood Technologies Plc* [2023] EWHC 250 at [82(e)] and [82(f)].

369 *Suisse Atlantique Société d'Armement Maritime SA v NV Rotterdamsche Kolen Centrale* [1966] 2 All ER at 92, see also *Pinewood Technologies Asia Pacific Ltd v Pinewood Technologies Plc* [2023] EWHC 250 at [82(e)] and [82(f)]. In *Hamblin v Moorwand Ltd* [2025] EWHC 817 (Ch) at [25(i)], the High Court held that a broad exclusion of both direct and indirect damages could not extend to a payment provider's duty to reinstate a customer. See also *Kudos Catering (UK) Ltd v Manchester Central Convention Complex Ltd* [2013] EWCA Civ 38 at [18]–[19] where Tomlinson LJ noted the lack of sanction for non-performance rendered the agreement "devoid of contractual content".

"cannot be used to avoid coming under any contractual obligations at all".[370] Yet that is exactly what Clause 12.1 purports to do.

315 If the Exclusions were effective, Cryptopia's customers would have only a $5,000 claim for certain narrow non-contractual (and non-tortious) claims. Such a claim would not be economically feasible in any court to enforce. The effect of reading and applying these clauses literally would be to give Cryptopia a free pass. This in itself is an abrogation of the ordinary legal right to compensatory damages for breach of duty.

316 Cryptopia was the fourth largest cryptocurrency exchange in the world. At the date of liquidation, it had over 2.2 million registered users worldwide.[371] Its extravagant terms and conditions were entirely unfit for the purpose of its business. Thousands of digital wallets were compromised during the Hack. The value of GNY's claim alone demonstrates that the purported limitation is, in practice, an effective exclusion of liability.[372] As is noted below, in New Zealand, caps of this nature are properly treated as attempts to contract out of statutory claims, in the same manner as total exclusion clauses.

(Ir)relevance of other platform terms

317 In his third affidavit, Mr Ruscoe includes examples of other terms and conditions from various other cryptocurrency platforms.[373] The terms include various limitations of liability. The Liquidators suggest that these other terms for other platforms are comparable to the Exclusions and therefore suggest that the Exclusions should not be considered to be onerous.[374]

318 This approach is misconceived. A similar argument was made and rejected in *Blu-Sky Solutions*. The Court accepted that the provisions similar to those before the Court were widespread in the telecommunications industry. However, that did not "of itself mean

---

370 Matthew Barber, Stephen Todd, *Burrows, Finn and Todd on the Law of Contract in New Zealand* (LexisNexis, online ed, 2022) at 258. See also *Suisse Atlantique Société d'Armement Maritime SA v NV Rotterdamsche Kolen Centrale* [1966] 2 All ER.

371 Ruscoe I, 31 July 2025, at [6]; [**201.0023**] at [**201.0025**].

372 See below at [**481**].

373 Ruscoe III, 23 April 2026, DIR3-1 – 77; [**401.0026**] at [**401.0038**] to [**401.0115**].

374 Liquidators' Submissions, [8.62].

that they are not onerous" and that such a fact could not "hold much weight".[375]

319 The reasoning in *Blu-Sky Solutions* is sound. An industry may adopt onerous clauses across the board. The law will still require that those onerous clauses are sufficiently drawn to the attention of counterparties. Whether a clause is "onerous" is a question of the legal effect of the clause, not a question of whether the clause is in common use. So reference to the approach of other exchanges is irrelevant to the matter before the Court for decision.

320 In any event, none of the clauses referred to by the Liquidators have been tested in the courts (let alone under New Zealand law or the law of a comparable jurisdiction). We do not have any information about how those clauses were incorporated into contracts for users, or about the applicable platforms.

321 In any event, the clauses in the terms and conditions attached to Mr Ruscoe's affidavit illustrate the draconian effect of Cryptopia's Exclusions, particularly insofar as it concerns Cryptopia's purported liability cap:

321.1 the Binance and Kraken terms and conditions cap liability at fees paid for the immediate 12 months preceding the event;[376]

321.2 the Coinbase terms and conditions limit liability to the value of the supported digital currency in the user's account;[377] and

321.3 the cited terms and exclusions all have generic exclusion terms for most claims that specifically preserve all non-excludable claims, as well as jurisdictional disclaimers. Cryptopia is alone in seeking to limit the application of statutory relief (the effect of cls 12.1(c) and 12.1(d) on s 43 of the FTA) and does not preserve other non-excludable claims (e.g. FMCA claims).

---

375 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [101]–[109].

376 Ruscoe III, 23 April 2026, DIR3-4 – 43; [**401.0026**] at [**401.0042**] to [**401.0081**].

377 Ruscoe III, 23 April 2026, DIR3-15; [**401.0026**] at [**401.0053**].

322 Each of these clauses are more tailored, and responsive, to user circumstances, than Cryptopia's blanket Exclusions.

Cryptopia gave account holders insufficient notice of the Exclusions

323 Account holders (including GNY) did not receive sufficient notice of the Exclusions, and they were not incorporated into Cryptopia's Terms & Conditions.

324 On account creation, the Terms & Conditions were hyperlinked in minute text above an acknowledgement box. That is the sole interaction account holders who established accounts after August 2018 ever had with them. There were no repeated opportunities to view and agree to them as was the case in *BBX Financial Solutions.*[378] There was no requirement to view, or further "clickwrap" acceptance required for subsequent updates: hardcopies were not offered, and summaries were not presented as in *Parker-Grennan*.[379] Cryptopia's approach is analogous to *Green v Petfre (Gibraltar) Ltd (t/a Betfred)* — an acceptance box was clicked and the Terms and Conditions were thereafter relegated to irrelevance.

325 The reasoning in *Green* (which endorsed *Spreadex*) is applicable. It would be irrational, on Cryptopia's behalf, to assume that account holders had read, appreciated, and agreed to sweeping Exclusions by clicking a single "I accept" box next to hyperlinked small text, which did not provide any notice of the nature of the onerous clauses contained within that link.[380] Moreover, on the (one) occasion when Cryptopia did communicate with account holders to attempt to explain elements of its Terms and Conditions, via its updating email in August 2018 in which it advised it had amended its terms (including to incorporate the Exclusions), it did so in a manner which, as in *Blu-Sky,* obfuscated the effect of the Exclusions.[381]

---

378 *BBX Financial Solutions Pty Ltd v Wallace* [2011] NZCA 667 at [26]–[27].
379 *Parker-Grennan v Camelot UK Lotteries Ltd* [2024] EWCA Civ 185 at [26], [48] and [49].
380 *Green v Petfre (Gibraltar) Ltd (t/a Betfred)* [2021] EWHC 842 (QB) at [25] and [167], *citing Spreadex Ltd v Cochrane* [2012] EWHC 1290 at [21].
381 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [110]. Also, see discussion above at [**284**]–[**287**].

326 The onerous nature of the Exclusions could and should have been brought to account holders' attention. In *Blu-Sky*, the Judge noted the terms could have been included with the order form, or sent separately with a prominent heading explaining their effect.[382] Cryptopia's clickwrap box could have required account holders to open, scroll and confirm their understanding of the Terms and Conditions, but it did not. Or it could have summarised or highlighted the fact of the Exclusions without needing a click through, so account holders were on notice of their general effect. Or the Terms and Conditions could have been sent separately to account holders by email on account creation, along with explicit notice of the nature of the Exclusions. Cryptopia did not take any of these steps.

Cryptopia gave GNY insufficient notice of the Exclusions

327 All of the reasoning above concerning account holders generally applies with equal force to GNY. In the case of GNY, however, Cryptopia had a range of other opportunities to draw GNY's attention to the Exclusions, but did not do so.

328 The Exclusions could have been drawn to GNY's attention with the Listing Quote, but were not. The Exclusions could have been drawn to GNY's attention in the Listing Contract, but were not. The Exclusions could have been explained in email correspondence with GNY, or attached to that correspondence, but were not.

329 Moreover, the fact of GNY being a business, and engaging with Cryptopia on a commercial basis, is largely irrelevant given:

329.1 Cryptopia's terms were non-negotiable and not drawn to GNY's attention. The terms were presented to GNY via clickwrap just like every other Cryptopia account holder;

329.2 GNY, like other Cryptopia account holders, is based offshore, and was not legally advised when engaging with Cryptopia;[383] and

329.3 the Exclusions are not "front and centre" in the terms: they are found on page 11 of a 16 page contract, and headed

---

382 *Blu-Sky Solutions Limited v Be Caring Ltd* [2021] EWHC 2619 (Comm) at [110].
383 See discussion at [**200**] above.

"Liability, Indemnities and Force Majeure" rather than under a more direct header such as "Exclusion of Cryptopia's Liability to Users": account holders would have to look hard to find the Exclusions, and actually read and understand the lengthy clause 12.1 to understand what the Exclusions meant. To illustrate the unreality of that step: the Liquidators' Submissions devote close to 5 pages to interpreting clause 12.1, indicating legal knowledge and skill is required for the task.[384]

330 As a result, the Exclusions were not incorporated into the Terms and Conditions, and are not enforceable against GNY (or any other account holder).

The Exclusions and GNY's fiduciary duty claim

331 Even if the Exclusions were effectively incorporated into Cryptopia's Terms and Conditions, and are prima facie enforceable, the actual effect of the Exclusions on each of GNY's non-contractual and non-tortious claims needs to be considered individually.

332 It does not appear that the Liquidators consider the Exclusions to apply to a claim for breach of fiduciary duty. The Liquidators' submissions on the exclusion clauses in places suggest that the Liquidators may consider the Exclusions to preclude this form of claim,[385] but elsewhere their submissions appear to accept that "the exclusion and limitation clauses would not apply" to a breach of a trustee's "irreducible core" of duties, including the duty to act honestly and in good faith.[386]

333 GNY agrees that, notwithstanding their apparent extremely wide scope, and even assuming the Exclusions were incorporated into the Terms and Conditions as a matter of law, the Exclusions nonetheless could not exclude Cryptopia's liability for breach of fiduciary duty. This is because, without the irreducible core of trust duties, there can be no trust.[387]

---

384 Liquidators' Submissions, 67-72.
385 See, for example, Liquidators' Submissions at [8.51] and [8.54].
386 Liquidators' Submissions, [7.11].
387 This parallels with the comments of Lord Wilberforce on purported total exclusions of contractual liability is clear, and reinforces why the Exclusions are unenforceable generally: *Suisse Atlantique Société d'Armement Maritime SA v NV Rotterdamsche Kolen Centrale* [1966] 2 All ER at 92.

334 In any event, the law requires express and clear words to preclude a trustee's liability for any breach of trustee obligations.[388] The Exclusions do not mention trustee obligations at all (and neither does the Risk Statement, for that matter). Moreover, the law precludes contracting out of fraud, and a breach of a duty of good faith and honesty is a species of equitable fraud.[389]

The Exclusions and GNY's FTA claim

335 Even if the Exclusions were effectively incorporated into GNY's Terms and Conditions, they would not be effective to contract out of the FTA.

FTA remedies expressly preserved

336 The Exclusions preserve account holders' FTA claims. The Liquidators suggest there is "no issue" that the Exclusions nonetheless amount to an agreement to contract out of the FTA, because of the application of the $5,000 liability cap in clause 12.1(d).

337 However, it is not clear whether the Exclusions purport to contract out of the FTA at all, including by way of clause 12.1(d). On its face, the Exclusions preserve GNY's FTA claim in full, including with respect to *any remedy*, per cl 12.1(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.
>
> (emphasis added).

338 This is the kind of textual ambiguity which tells against an interpretation that would vitiate valuable rights. Clause 12.1(d) applies a liability cap "notwithstanding" cl 12.1(c). This language is not reconcilable with the express preservation of any FTA remedy in cl 12.1(c). To the extent cl 12.1(d) clashes with cl 12.1(c), that ambiguity should be construed against Cryptopia, and the exclusion disallowed to FTA and CGA claims.[390]

---

388 *Cooper v Pinney* [2024] NZSC 181, [2024] 1 NZLR 935 at [120].
389 *L'Estrange v Graucob* [1934] 2 KB 394. See *Armitage v Church* HC Wellington CIV-2009-485-1952, 27 May 2011 at [187]–[195].
390 *Ferrer-Aza v NZONE Race Management Ltd* [2016] NZHC 885 at [37]. Matthew Barber, Stephen Todd, *Burrows, Finn and Todd on the Law of Contract in New Zealand* (LexisNexis, online ed, 2022) at 242–243.

FTA remedies are not excluded

339 Alternatively, if the Exclusions, properly interpreted, did purport to contract out of FTA liability, GNY agrees with the Liquidators that the effectiveness of that attempt would fall to be considered under ss 5C and 5D of the FTA.[391] This is because liability caps such as Clause 12(d) purport to override the remedies available under s 43 of the FTA, and therefore amount to a contracting out of the FTA.

340 The starting position is that contracting out is ineffective: s 5C. There is an exception for parties "in trade" (which both GNY and Cryptopia were) but this exception is subject to the requirements in s 5D(3) being met. Of those requirements, the primary question is whether it is "fair and reasonable" that the Exclusion in clause 12.1(d) applies per s 5D(3)(d).

341 There are several reasons why it is not fair and reasonable for the Exclusions to apply — including all of the factors in section 5D(4) pointing to this conclusion:

341.1 section 5D(4)(a): refers to the subject matter of the agreement. The subject matter is cryptocurrency trading amongst international participants with no expectation of knowledge or understanding of New Zealand law. Although GNY is in trade, most account holders would not be, and all account holders were subjected to the same account sign up process, and the same clickwrap "one and done" approach to Cryptopia's Terms and Conditions;

341.2 section 5D(4)(b): refers to the value of goods, services or interests in land. GNY had substantial holdings on the platform across two accounts.[392] The purported $5,000 liability cap is completely out of step with GNY's holdings. It is also completely out of step with the payments made by GNY to Cryptopia for services (its listing fee, for example, exceeds the liability cap by a factor of 8x to 10x depending on when you calculate the indirect exchange rates).[393] Indeed, it

391 Liquidators' Submissions, [8.76].

392 [redacted] 30 March 2025, [redacted]2 – 3; [**201.0001**] at [**301.0077**] to [**301.0078**].

393 The listing fee was around 6.16627 BTC in November 2018, see [redacted] 30 March 2025, at [12]; [**201.0001**] at [**201.0003**]. This amounted to N[redacted],000 - $50,000 at the time. Note further that Cryptopia required GNY to operate "level 2" verified accounts to list LML, permitting NZD $50,000 in trading every 24 hours:

is out of step with Cryptopia's entire product offering and position as the world's fourth-largest cryptocurrency exchange;

341.3 section 5D(4)(c): refers to the respective bargaining powers of the parties. The Exclusions were standard form, non-negotiable, and implemented without being drawn to GNY's attention.[394] In terms of matters the FTA specifically directs us to consider: GNY had no scope to negotiate the Exclusions (per s 5D(c)(i)) and GNY was required to either accept or reject the Exclusions (per s 5D(C)(ii));

341.4 section 5D(d): refers to the extent to which Cryptopia "knew that a representation made in connection with the agreement would", but for the Exclusion, have breached a core liability provision of the FTA, including s 13: as explained earlier, Cryptopia did know that its cybersecurity settings were neither safe nor secure when it implemented the Exclusions in August 2018.[395] Moreover, while the Liquidators emphasise the Risk Statement[396] made clear that trading on a cryptocurrency exchange is a speculative and inherently risky activity,[397] the relevance of that point to contracting out of the FTA is not obvious: the Risk Statement is addressed to generic industry risks. It did not disclose the "risk" that Cryptopia might make misleading or deceptive statements about its services. That is a fundamentally different risk to general trading risks of the kind addressed in the Risk Statement. Even then, it is not safe to assume that any account holders were actually aware of the Risk Statement, given the obscure way in which it was made available - either by website fine print link,[398] or indirect link incorporated on

---

Sibenik I, 1 August 2025, PJS1-27 [**201.0090**] at [**302.0747**]; and Brocket I, 27 November 2019, TJSB1-42; [**401.0194**] at [**401.0242**].

394 As described above at [**56**]–[**61**].

395 See above at [**143**]–[**160**].

396 Note again that the Risk Statement was not actually provided to an account holder signing up to a Cryptopia account - other than by way of link provided in the Terms and Conditions which themselves were only provided by link.

397 Liquidators' Submissions, [8.81].

398 Ruscoe I, 31 July 2025, DIR1-110; [**201.0023**] at [**301.0427**].

page 10 of the Terms & Conditions, in the middle of clause 7 at clause 7.1(a)(v);[399] and

341.5 section 5D(e): refers to whether parties "received advice from or were represented by a lawyer, either at the time of the negotiations leading to the agreement or at any other time". GNY was not. The Liquidators refer to an email sent by [redacted] in which he notes GNY was represented by Carey Olsen, and infer that GNY "communicated it was legally represented by international law firm Carey Olsen".[400] This is a misread of the email in question (and not a reasonable inference from it): Carey Olsen is not a New Zealand law firm, and GNY communicated to Cryptopia that it was represented by Carey Olsen with respect to its Jersey-based Initial Coin Offering (**ICO**) (a link to the nature of the instruction was included in the email). All of GNY's communications with Cryptopia were with GNY team members directly, with no involvement by Carey Olsen.

342 Stepping back, while it is fair for the Liquidators to describe GNY as a "sophisticated commercial party that voluntarily chose to use the Platform",[401] GNY's position in connection with the Exclusions is the same as any Cryptopia account holder, including individuals: it had no capacity to negotiate, the terms were "signed" in a once over lightly clickwrap context, in circumstances where the Exclusions were not drawn to its attention. It is difficult to see how GNY being "in trade" in and of itself is sufficient for section 5D to be engaged, given this is simply a threshold matter for section 5D to be considered, and all of the substantive factors in that section militate against it being "fair and reasonable" for the Exclusion to apply.

The Exclusions and GNY's FMCA claim

343 The Liquidators accept that Cryptopia cannot contract out of the FMCA.[402] GNY's FMCA claim is unaffected by the Exclusions.

---

399 Brocket I, 27 November 2019, TJSB1-10; [**401.0194**] at [**401.0213**].
400 Liquidators' Submissions, [8.80]. Sibenik I, 1 August 2025, PJS1-15; [**201.0090**] at [**302.0718**].
401 Liquidators' Submissions, [8.80].
402 Liquidators' Submissions, [8.169].

The Exclusions and GNY's CGA claim

344 Finally, the exception to the CGA's application under s 43(2) is not made out. Section 43(2) allows contracting out of the CGA for "business transactions", provided certain criteria in ss 43(2) and 43(2A) are made out for transactions of this kind. Those criteria are identical to the criteria in s 5D of the FTA, and the same analysis applies.

SECTION 8: BTC DETERMINATION & PAYMENT

345 GNY's claim should be determined in BTC and satisfied by 'in specie' distribution of BTC held by the Liquidators.[403] GNY's claim should not be, as the Liquidators propose, converted into NZD and met by converting existing BTC into NZD.

346 It now appears to be common ground that the date for valuing GNY's loss is the date of the Hack.[404] GNY therefore does not address that point further.

347 In summary:

347.1 Section 306(2) of the Companies Act does not apply because GNY's claim is not a foreign currency claim. GNY's claim, properly quantified in BTC, does not need to be converted into NZD.

347.2 The Court thus has a discretion on how to proceed with the determination and payment of GNY's claim. Those issues must be addressed by a combination of first principles and other statutory provisions.

347.3 In the present case there is room for considering specific circumstances and the exercise of appropriate judgement to order an in-specie distribution instead of conversion to and payment in NZD.

347.4 The Court may properly determine GNY's claim in BTC and order the Liquidators to distribute BTC in specie directly to GNY in satisfaction of GNY's claim, in light of:

(a) the Liquidators' duty to distribute assets in a "reasonable and efficient" manner under s 254;

(b) the Court's broad power to supervise and direct liquidators under s 284;

---

403 **Section 9** below separately addresses the proper valuation of GNY's claim, by reference to expert valuation evidence.

404 Liquidators' Submissions, [8.286]–[8.291].

347.5 In the present case, the claim is properly quantified and determined in BTC, and is properly met by in-specie distribution of available BTC, in circumstances where:

(a) there is a real link between GNY's claims and BTC, given that BTC was the natural counterpart for a new cryptocurrency in LML, and LML was traded for BTC in almost all trades; and

(b) GNY at all relevant times sought payment from Cryptopia in BTC, and based on a valuation of LML in BTC.

Section 306(2) does not apply - BTC is not a "foreign currency"

348 Section 306(2) does not apply to GNY's claim because digital assets such as BTC cannot properly be construed as "currency". GNY's claim in BTC is therefore not a "foreign currency" claim.

349 Whether digital assets can qualify as "currency" (or "money") in the context of insolvency law was well-summarised by the UK's Ministry of Justice UK Jurisdiction Taskforce (**UKJT**) 2024 Legal Statement on Digital Assets and Legal Insolvency Law (the **UKJT Legal Statement**).[405] Of particular note:

> [66] An obligation to pay (or deliver) a specific quantity of digital assets does not satisfy that requirement because digital assets cannot be treated as money, at least not yet. In Miller *v Race* Lord Mansfield said that what is treated as money "by the general consent of mankind" is given "the credit and currency of money to all intents and purposes". Digital assets, even where used as a means of payment, do not yet have such credit and currency. The value of digital assets "depends on different structural and social concepts compared to existing fiat currencies" and all digital assets (including stablecoins) fluctuate in value against fiat currencies. The holder of a digital asset has no legal right to exchange that digital asset for any specific fiat currency. Many obligations that specify a certain quantity of digital assets require delivery or repayment of the digital asset in question and cannot be recharacterised as a monetary obligation or a debt for a liquidated sum of money. The "core" legal obligation in respect of a quantity of digital assets "owed" by a company or bankrupt is one of delivery of those digital assets, rather than payment of a monetary sum. An action to enforce such an obligation would therefore be

405 UK Jurisdiction Taskforce *Legal Statement on Digital Assets and English Insolvency Law* (The LawTech Delivery Panel, May 2024). His Honour Gendall J, in a prior 2020 judgment relating to Cryptopia, had relied on a (different) paper published by the UKJT: *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728 at [12], [64], [88], [102], [121] and [131], citing UK Jurisdiction Taskforce *Legal Statement on Cryptoassets and Smart Contracts* (The LawTech Delivery Panel, November 2019).

> characterised or construed as a claim for unliquidated damages for failure to deliver, rather than as a monetary debt.
>
> …
>
> [80] We consider the question of whether or not an obligation to deliver digital assets is a debt owed in a "currency" to be the same as the question as to whether or such assets amount to 'money'. Further, for the reasons outlined above,52 we think that digital assets are not (yet) 'money' (or, therefore, "currency" for the purposes of Rule 14.21), but that one or more forms of digital assets may become "currency" at some point in the future, if and when they are (as a matter of fact) commonly and continuously accepted as a means of exchange or a unit of account.
>
> (references omitted)

350 The UKJT analysis applies equally in New Zealand, to s 306(2), particularly given the substantial similarity of Rule 14.21 of the Insolvency Rules (England and Wales) 2016 (to s 306(2) of the Companies Act.

351 A finding that crypto-assets are neither "money" nor "currency" would also be consistent with New Zealand law outside of the insolvency context:

351.1 Section 4 of the Limitation Act 2010 defines money as currency that is or has been authorised as a medium of exchange by the law of New Zealand, or any other country.

351.2 Section 16 of the Personal Property Securities Act 1999 repeats the above.

351.3 The IRD treats cryptocurrency as personal property for tax purposes — not currency. Cryptocurrency is also not recognised as currency for the purposes of the Goods and Services Tax Act 1985 or the Income Tax Act 2007.[406]

352 Several decisions from comparable jurisdictions have found that cryptocurrencies are not money or currency:

352.1 In *Quoine Pte Ltd v B2C2 Ltd,* the Singaporean Court of Appeal held, while cryptocurrencies have the fundamental characteristics of intangible property: "[c]ryptocurrencies are

---

406 Inland Revenue "Impact Summary: Tax treatment of cryptocurrencies" (31 May 2021) <https://www.regulation.govt.nz/assets/RIS-Documents/ria-ird-ttc-may21.pdf>.

not legal tender in the sense of being a regulated currency issued by a government...".[407]

352.2 In *Florida v Espinoza,*[408] Florida's Third District Court of Appeal noted there was "no dispute" that Bitcoin was not currency under Florida's legislation, finding instead that it was a "payment instrument".[409] The statutory language was clear that "monetary value" was not synonymous with "currency".

352.3 Three decisions from the United Kingdom preceded the statutory introduction of a third kind of property that cryptocurrency may fall under – none held that cryptocurrency qualified as money or currency in the usual sense.[410]

353 Moreover:

353.1 The Reserve Bank of Australia has stated in guidance that cryptocurrencies are not money because:[411]

(a) They are not a widely accepted means of payment (and this remains true despite the guidance being published around 2021).

(b) Large fluctuations in the price of many crypto-assets mean that their purchasing power is not maintained over time, reducing their effectiveness as a store of value.

(c) Cryptocurrencies are not yet an effective unit of account in Australia. Goods and services remain, largely, priced in Australian dollars.

353.2 The United Kingdom recognises cryptocurrency as personal property.[412] The United Kingdom's Law Commission, in its

---

407 *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 2 [*B2C2* (SGCA)].
408 *Florida v Espinoza* (Fla. 3d DCA 2019).
409 At 16.
410 *AA v Persons Unknown* [2019] EWHC 3556 (Comm); *Osbourne v Persons Unknown* [2022] EWHC 1021 (Comm); *Tulip v Bitcoin Association* [2023] EWCA Civ 83.
411 Reserve Bank of Australia "Digital Currencies" (2021) <https://www.rba.gov.au/education/resources/explainers/pdf/cryptocurrencies.pdf?v=2026-03-24-15-31-30>.
412 Property (Digital Assets etc) Act 2025 (UK).

report that this legislative development came out of, found cryptocurrencies are "currently unlikely to be (or to be treated as) money in the same way as fiat currency".[413] The Commission noted:

(a) cryptocurrencies are "self anchored mathematic creatures", the value of which depends on different structural and social concepts compared to existing fiat currencies;[414] and

(b) holding a crypto-token, in itself, generates no right to exchange that token for legal tender.[415]

Court has broad discretion on determination and payment of GNY's claim

354 The Court is empowered under s 284 of the Companies Act to both determine GNY's claim in BTC, and to order an in-specie distribution of BTC in satisfaction of GNY's claim.

355 Under s 284(1), the Court may "give directions in relation to any matter arising in connection with the liquidation". That is a broad power which is capable of including both determination of creditor claims, as well as directions on distribution (addressed in more detail later in these submissions).

356 The Court's discretion is broad, with the Court able to make any orders necessary to enable a liquidation to proceed pragmatically, effectively and efficiently to both realise the company's assets and to distribute the net proceeds to creditors.[416]

357 In determining whether to exercise its discretion to give directions under s 284, the Court will consider the particular circumstances of

---

413 Law Commission (UK) *Digital assets* (HC 1486, Law Com No 412, June 2023) at [9.9].

414 B Geva and D Geva "Non-State Community Virtual Currencies" in D Fox and S Green (eds) *Cryptocurrencies in Public and Private Law* (online edition, Oxford, 2019) at [11.56].

415 Per a footnote in the Law Commission (UK) report (at n 1035): "At least in England and Wales and other jurisdictions that have not adopted certain crypto-tokens as legal tender. 'Legal tender' is usually taken to refer to the banknotes or coins which constitute the national currency issued under the legislation of the State", S Green, "'It's Virtually Money" in D Fox and S Green (eds) *Cryptocurrencies in Public and Private Law* (online edition, Oxford, 2019) at 2.31–2.33".

416 *Re Fisk* [2018] NZHC 2007 at [81]; *Re Roslea Path Ltd* (in liq) [2013] 1 NZLR 207 (HC) at [112].

the liquidation, and how the liquidators should respond to their duties in those circumstances.[417]

358 In the present context, circumstances justify the Court determining GNY's claim in BTC and ordering the Liquidators to make an in specie distribution of BTC to GNY in satisfaction of its claim.

GNY's claim is properly determined by reference to BTC

359 GNY does not seek to have its claim quantified, determined and paid in BTC as a matter of expediency. Determining and paying the claim by an in-specie distribution of BTC (rather than converting BTC to pay in NZD) is appropriate in the present case.

360 The High Court of Singapore in *Fantom Foundation Ltd v Multichain Foundation Ltd*[418] has previously addressed the inherent complexity and uncertainty of ascertaining the market value of cryptocurrency at a given point in time (as addressed in more detail in Section 9). Relevantly, the High Court:

360.1 acknowledged that "cryptocurrencies are conventionally traded using other cryptocurrencies" (rather than fiat currencies);[419]

360.2 found that the appropriate approach to valuing lost cryptocurrency is by reference to the token it is "most liquidly traded against".[420]

361 That approach is both principled and sensible. Otherwise, there is the risk of the conversion process not only eroding, but fundamentally distorting, value.

362 Under that test, LML is properly valued by reference to BTC. LML was paired with BTC in almost all LML trades prior to the Hack. The trading data collated by the Liquidators' and their staff shows that 95.7% of the LML tokens traded prior to the Hack were exchanged

---

417 *Re Waller* HC Auckland CIV-2005-404-7051, 26 July 2006 at [22].
418 *Fantom Foundation Ltd v Multichain Foundation Ltd* [2024] SGHC 173.
419 *Fantom Foundation Ltd v Multichain Foundation Ltd* [2024] SGHC 173 at [37].
420 *Fantom Foundation Ltd v Multichain Foundation Ltd* [2024] SGHC 173 at [28].

by the seller for BTC.[421] The remaining 4.3% of LML was traded for alternative cryptoassets called "LTC" and "Dogecoin".

363 Given that pairing history, GNY has at all times articulated its claim against Cryptopia in BTC:

363.1 Post-hack, GNY engaged in prolonged correspondence seeking information and attempting to stop the trading of stolen LML tokens on Bitbay.[422] On 18 March 2018, GNY advised Cryptopia that it would be prepared to resolve its claim for loss if Cryptopia paid GNY 443 BTC.[423] Cryptopia did not respond to that proposal.

363.2 On 10 July 2019, GNY submitted its claim in the liquidation of Cryptopia, which was quantified in BTC (and then further converted to NZD).[424]

363.3 In September 2019, GNY (via counsel) wrote to the Liquidators explaining that the LML-related loss was properly tied to BTC. Specifically:[425]

(a) comparing the value of a cryptocurrency against Bitcoin is common, and provides a more authentic assessment of value than comparing a cryptocurrency to a fiat currency. This is consistent with the High Court of Singapore's findings set out above; and

(b) when GNY listed its LML tokens on the exchange platform, Cryptopia gave GNY the LML:BTC pairing, and quoted the LML price in BTC. As above, LML was subsequently traded for BTC in almost all trades.

363.4 The draft amended statement of claim filed with GNY's notice of opposition states GNY lost 15,409,316.7196351 LML, with the value of that LML being 491.24901703 BTC at the date of the hack. The amended statement of claim then quantifies

---

421 O'Shea I, 22 December 2025, Appendix F.2; [**304.1476**] at [**304.1561**].
422 [redacted] 30 March 2025, at [16]–[18]; [**201.0001**] at [**201.0004**].
423 L[redacted]rom GNY to Cryptopia re recovery of funds, 18 March 2019; [**302.0887**].
424 Letter from GNY counsel to Liquidators' counsel re GNY's unsecured creditor claim, 10 July 2019; [**302.0949**].
425 Letter from GNY counsel to Liquidators' counsel re requests for information, at [72]; [**302.0959**] at [**302.0972**].

GNY's total losses, as a result of the hack, to be 3,505.81528703 BTC.[426]

364 Assessing GNY's loss in BTC is the best measure because the nature of GNY's loss was uniquely tied to BTC being the de facto conversion currency for LML. If cryptocurrency held by a company in liquidation is closely linked to relevant losses (concerning a related cryptocurrency), then it follows that one must carefully consider whether the right way of valuing and responding to the claim is through an in-specie distribution in BTC rather than an NZD conversion (addressed further below).

365 In the present case, LML could not be traded directly for NZD. Any attempt to value GNY's hack losses by reference to NZD necessarily involves an implicit further translation step of valuing LML in some other currency, such as USD, in order to convert that currency to NZD. Such an artificial, roundabout, process inevitably loses something in translation.

366 Contrary to the Liquidators' submissions, the present case has no parallel to the English Court of Appeal's judgment in *BSV Claims v Bittylicious*.[427] That is not a case in which a claimant sought to value their claim by reference to another cryptocurrency. Rather, the claimants claimed "foregone growth" losses in respect of tokens to which they had lost access, on the basis that the tokens would have experienced comparable growth in value to BTC. It is in that context that the Court ruled that the claimants were not entitled to "argue that their losses should be assessed by reference to the value of some other better-performing cryptocurrency at some future unspecified date". The hypothetical claims at issue in that judgment are not comparable to GNY's claim and do not assist on the question of valuing GNY's loss.

---

426 GNY's amended statement of claim dated April 2025, annexed to Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025; [**101.0016**] at [**101.0038**].

427 *BSV Claims v Bittylicious* [2025] EWCA Civ 661.

In specie distribution consistent with Liquidators' duties

367 Section 253 of the Companies Act provides:

> Subject to section 254 of this Act, the principal duty of a liquidator of a company is—
>
> (a) To take possession of, protect, realise, and **distribute the assets**, or the proceeds of the realisation of the assets, of the company to its creditors in accordance with this Act; and
>
> (b) If there are surplus assets remaining, to distribute them, or the proceeds of the realisation of the surplus assets, in accordance with section 313(4) of this Act—
>
> in **a reasonable and efficient manner**.
>
> (emphasis added)

368 The provision reflects the common law position and the principal duty of a liquidator.[428]

369 In performing their duties under s 253, liquidators must observe the rules set out in ss 303–313 of the Companies Act (addressed further below).[429] For the reasons above, s 306(2) does not apply in the present case.

370 Section 253 expressly acknowledges the liquidators' ability to both "*distribute the assets*" and to distribute "*the proceeds of the realisation of the assets*". It allows for the distribution of assets in-specie.[430] Liquidators are empowered to decide whether to realise assets to distribute the proceeds, or just distribute in-specie. What matters in making that decision is that the liquidators must exercise their duties and power in "*a reasonable and efficient manner*". That reflects the common law requirement that a liquidator must, in carrying out of the duties of a liquidator, "*display that degree of skill and care which, by accepting office, he has held himself out as possessing*".[431]

371 By way of comparison, under r 14.13 of the Insolvency Rules (England and Wales) 2016, administrators and liquidators are

---

428 Law Commission *Company Law: Reform and Restatement* (NZLC R9, 1989) at [667]–[670].

429 Linda Howes and Stephen Revill *Company Law* (online ed, Thomson Reuters) at [CA253.02(1)].

430 Linda Howes and Stephen Revill *Company Law* (online ed, Thomson Reuters), at CA253.02(1)

431 Linda Howes and Stephen Revill *Company Law* (online ed, Thomson Reuters), at [CA253.02(2)], citing J O'Donovan *McPherson: The Law of Company Liquidation* (3rd ed, Sydney, Law Book Co, 1987) at 218.

enabled to divide property which "from its peculiar nature or other special circumstances cannot be readily or advantageously sold" among the company's creditors in its existing form. That can only be done with the permission of the creditor committee or, if there is no such committee, the creditors themselves. The UKJT Legal Statement observed that the r 14.13 principles "should enable the division and distribution of digital assets if necessary".[432]

372 While there is no direct equivalent to r 14.13 under New Zealand law, s 253 gives a broad power to liquidators to act as needed to ensure reasonable and efficient distribution in satisfaction of creditors' claims.

373 Nothing in the Companies Act would prevent in specie distribution of BTC. While the Act does not define the term "assets", "property" has a wide definition.[433] Cryptocurrencies have been characterised as intangible personal property under that definition.[434] BTC is an asset for the purpose of s 253.

374 The Courts have previously approved in-specie distributions (including in the cryptocurrency context) where practicality and fairness considerations merited it. Specifically:

374.1 The Hong Kong Court of First Instance in *Re Gatecoin Limited*[435] found that an in-specie distribution by liquidators of cryptocurrency assets to claimants (albeit ones found to have a beneficial interest in cryptocurrency held on trust) were appropriate, unless:[436]

(a) costs of doing so were prohibitive; or

(b) the customer preferred cash; or

(c) there was a shortfall of assets relative to claims; or

---

432 UK Jurisdiction Taskforce *Legal Statement on Digital Assets and English Insolvency Law* (The LawTech Delivery Panel, May 2024) at 26.
433 Companies Act 1993, s 2.
434 *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728.
435 *Re Gatecoin* [2025] HKCFI 493. This judgment followed a prior decision determining whether the relevant cryptocurrency was held on trust by Gatecoin, a cryptocurrency exchange, for the benefit of its customers, and whether cryptocurrency is property: *Re Gatecoin* [2023] HKCFI 914.
436 *Re Gatecoin* [2025] HKCFI 493 at [32]-[37].

(d) it was otherwise impractical.

374.2 In *Longley,*[437] the Federal Court of Australia permitted in-specie distribution by a liquidator to certain creditors of shares in another company. The shares were in the company that had purchased assets from the company in liquidation, and were provided as part-consideration for the sale of those assets. Because of a "holding lock" preventing the sale of some of the shares, it was more efficient and practical to distribute the shares in specie to the relevant creditors rather than incur the ongoing costs of the liquidation while waiting to sell the shares. The creditors had agreed to receive the shares in specie in satisfaction of their claims. There was nothing in the Corporations Act that rendered an in-specie distribution invalid or contrary to public policy.[438]

374.3 The Supreme Court of New South Wales in *Re HIH Services Pty Ltd* cited *Longley* in approving an in-specie distribution of the company's only asset: a right to prove its claim in the liquidation scheme of arrangement of another group company. The recipient of this distribution was the sole creditor.[439] The Court noted considerable savings in proceeding this way, compared to the cost of the liquidator attempting to realise the asset.[440]

In specie distribution of BTC is practical and not prejudicial

375 An in specie distribution of BTC in satisfaction of GNY's claim is a practical and appropriate approach consistent with the cases cited above:

375.1 There is no evidence suggesting that the costs of making an in specie distribution of BTC to GNY would be prohibitive.

---

437 *Longley & anor v ACN 090 609 868 Pty Ltd (in liq) (formerly Solar Systems Pty Ltd) & anor* [2010] FCA 1468, (2011) 81 ACSR 517.

438 *Longley & anor v ACN 090 609 868 Pty Ltd (in liq) (formerly Solar Systems Pty Ltd) & anor* [2010] FCA 1468, (2011) 81 ACSR 517 at [16]–[17].

439 *Re HIH Services Pty Ltd (in liq)* [2012] NSWSC 1188 at [1]–[5].

440 The Supreme Court of New South Wales similarly found practical considerations justifying in specie distributions of assets to shareholders: see *Re Allseal Floor Preparations Pty Ltd (in liq)* [2015] NSWSC 1990 and *Re Anne Lewis Pty Ltd* [2016] NSWSC 1860.

375.2 To the contrary, conversion of BTC into fiat currency is an unnecessary value-eroding step (and inconsistent with the liquidators' obligations to discharge their duties in a reasonable and efficient manner). An in specie distribution would avoid both the costs and fees associated with converting BTC into fiat currency, and the value erosion inherent in such a conversion process. Converting BTC into NZD may double the erosion of the value to the extent that BTC needs to be converted into USD before conversion into NZD.

375.3 GNY seeks, and has always sought, payment in BTC rather than fiat currency.

375.4 No creditor would be harmed by making an in specie BTC distribution to GNY, as unclaimed assets exceed creditor claims.

375.5 The Liquidators hold available surplus BTC that they can readily distribute to GNY.

Payment in full of GNY's claim in BTC is appropriate as a matter of policy given available assets

376 The Cryptopia liquidation is, at a minimum, analogous to a solvent liquidation. Unclaimed assets, if made available to meet creditor claims, appear to substantially exceed unsecured creditor claims (even accounting for asset claims made following the Hard Cut-Off Date).

377 As a matter of policy, in what is effectively a solvent liquidation, it is appropriate that GNY's claim be paid in full (in BTC without any conversion to fiat currency).

378 While s 306(2) does not apply to GNY's claim (for the reasons identified earlier), policy discussions in prior judgments dealing with s 306(2) and its equivalents are relevant to and animate this issue.

379 Section 306(2) is one of a number of sections intended to underpin the application of the *pari passu* principle fundamental to insolvency law. That is, in insolvent liquidations, where creditor claims exceed assets and proceeds available for distribution, all unsecured

creditors rank equally as amongst each other and receive distributions rateably.

380 The origins of s 306(2) can be traced back to the English Court of Appeal in *Re Lines Bros*.[441] The Court of Appeal, in dealing with the issue of foreign currency claims, found that foreign currency claims had to be converted to domestic currency claims as at the date of liquidation. That was necessary to ensure a like-for-like comparison of all claims, to enable company property is to be applied in satisfaction of a company's liabilities *pari passu.*

381 The majority of the UK Supreme Court more recently upheld that foreign currency claims must be converted to domestic currency as at liquidation in the *Lehman Brothers* case.[442]

382 We are, of course, not here dealing with a foreign currency claim, for the reasons set out above. The arguments around policy and principle regarding conversion of foreign currency claims remain contestable (with *Lehman Brothers* not yet applied in New Zealand).

383 What is not contestable, however, is the consistent throughline in all of the cases that the position is fundamentally different in the case of a solvent liquidation, where there may be surplus assets once provable debts are paid in full. Specifically:

383.1 the Court in *Re Lines Bros*, starting at 195, stated:

> …it may be relevant to observe that the view has been repeatedly expressed in relation to interest that, once the provable debts have been satisfied in full, so that the company has in that sense a surplus of assets, the duty of the liquidator is to discharge the contractual indebtedness of the company in respect of such debts to the extent that the contractual indebtedness exceeds the provable indebtedness.
>
> …
>
> It is on that principle that a creditor may claim post-liquidation interest. He does this on the basis that obligations under the contract are not necessarily discharged despite the fact that all provable debts have been paid at 100p in the pound. It may well be the duty of the liquidator, in the case of a wholly solvent liquidation, if a foreign currency creditor has been paid less than his full contractual foreign currency debt, to make good the shortfall before he pays anything to the shareholders. I do not say that this

---

441 *Re Lines Bros* [1983] Ch 1 (CA); Linda Howes and Stephen Revill *Company Law* (online ed, Thomson Reuters) [CA306.02].

442 *Re Lehman Brothers International* [2017] UKSC 38, [2018] AC 465.

> is necessarily the solution to the problem posed, but I have not heard any convincing objection to that solution.
>
> …
>
> I do not think, therefore, that a foreign currency creditor can base a claim on the depreciation in the cross rate between sterling and the foreign currency until the liquidator has assets in his hands which will otherwise go to the shareholders. At that stage, but not earlier, as it seems to me, it would be entirely just to allow the foreign currency creditor to recover the same amount as he would have been able to recover if no liquidation had ever taken place.

384 Subsequently, in the *Lehman Brothers* case, Lord Neuberger recognised that:[443]

> …it is hard to quarrel with the argument that if it turns out there is a surplus, it would be commercially unjust to distribute it to the members without first making good the shortfall suffered by the foreign currency debtor.

385 Although Lord Neuberger felt compelled by the relevant statutory provisions relating to foreign currency claims to convert to pound sterling, the point of principle was recognised. Lord Clarke, in dissenting, went further. His Lordship found that liquidation was primarily a procedural and administrative device to deal with circumstances of shortfall where claims exceeded assets. Mere provision of rules for the proof of foreign currency claims, which were undoubtedly necessary to facilitate a *pari passu* distribution in the case of insolvency, did not mean that Parliament intended to mandate that all such claims would be substantively compromised even in circumstances of solvency.[444] Clear statutory words would be required to deprive the creditor of its common law rights.[445]

Conclusion on determination and payment of GNY's claim in BTC

386 GNY's claim is not a foreign currency claim, and it therefore need not, a matter of statute, be converted into NZD. GNY submits, respectfully, that the Court should exercise its broad discretion under s 284 and both determine and order payment of GNY's claim in BTC. That is appropriate in circumstances where BTC is a natural counterpart to LML, substantial unclaimed BTC is held by the Liquidators and the distribution will not prejudice any other party.

---

443 *Re Lehman Brothers International* [2017] UKSC 38, [2018] AC 465 at [80].

444 *Re Lehman Brothers International* [2017] UKSC 38, [2018] AC 465 at [210]–[220].

445 *Re Lehman Brothers International* [2017] UKSC 38, [2018] AC 465 at [220]–[221].

387 That outcome will provide GNY with the outcome it always sought against Cryptopia: compensation reflecting the value of lost LML and lost market capitalisation in BTC as at the date of breach. To force GNY's claim to be understood in NZD rather than BTC is neither realistic nor fair.

SECTION 9: VALUING GNY'S CLAIM

Summary

388 The Court has been provided with two distinct valuations of GNY's claim, by experts engaged by GNY and the Liquidators respectively.

389 On the one hand, Mr Bruce O'Shea of KordaMentha Australia has prepared a comprehensive report setting out a valuation of GNY's claim in the range of hundreds of BTC. Mr O'Shea is an experienced and qualified valuer who has undertaken a ground-up valuation based on orthodox principles of:

389.1 Assessing a market value of an LML token based on available data for market trades between:

(a) GNY and a third party; and

(b) A third party and a third party,

while excluding internal GNY-GNY trades; and

389.2 In respect of the stolen token claim, multiplying the market value of a single LML token by the number of stolen LML tokens as at the date of the Hack, to get a base valuation;

389.3 In respect of the lost market capitalisation claim, calculating a base valuation that is the difference in market valuation of the 120 million of circulating LML tokens as at:

(a) 13 January 2019 (being the date of the Hack) and

(b) 30 May 2019 (being the date when the hacker stopped selling LML tokens and the impact of the Hack effectively ceased)

389.4 Applying a marketability discount to each base valuation, to reflect how readily the relevant parcel of LML tokens being valued could be sold on the market.

390 Using that methodology, Mr O'Shea has valued GNY's stolen LML token and market capitalisation claims as follows:[446]

Table 2: Range of value of stolen LML tokens

	At the date of the Hack			Around the date of my report	
Marketability discount range	Amount (BTC)	Amount (USD)	Amount (NZD)	Amount (USD)	Amount (NZD)
Value prior to marketability discount (0%)	482.75	1,766,312	2,586,870	41,611,432	72,129,586
Value with marketability discount applied of:					
30%	337.92	1,236,418	1,810,809	29,128,002	50,490,710
40%	289.65	1,059,787	1,552,122	24,966,859	43,277,752
50%	241.37	883,156	1,293,435	20,805,716	36,064,793

Source: KordaMentha (refer to Table 12 and Table 13 below)

Table 3: Range of value for the lost market capitalisation

	At the time the Hack is assumed to cease			At the date of my report	
Marketability discount range	Amount (BTC)	Amount (USD)	Amount (NZD)	Amount (USD)	Amount (NZD)
Value prior to marketability discount (0%)	3,553.60	30,780,452	47,250,725	306,309,132	530,958,681
Value with marketability discount applied of:					
60.0%	1,421.44	12,312,181	18,900,290	122,523,653	212,383,472
70.0%	1,066.08	9,234,136	14,175,217	91,892,740	159,287,604
80.0%	710.72	6,156,090	9,450,145	61,261,826	106,191,736

Source: KordaMentha (refer to Table 14, Table 15 and Table 16 below)

391 GNY submits that the Court ought to apply the lower end of the marketability discount range to each claim, giving a final value of:

391.1 337.92 BTC for the stolen LML tokens claim; and

391.2 1,421.44 BTC for the lost market capitalisation claim.

392 The other valuation has been provided by Mr Sibenik for the Liquidators. Mr Sibenik is not a valuer, and has not undertaken a ground-up valuation like Mr O'Shea. Mr Sibenik concludes that the LML tokens GNY issued, and in turn GNY's claims, were and are essentially worthless.

393 An important part of this trial will be for the Court to test and assess the assumptions made by each expert in coming to those very different views. GNY will address this further in closing, but at this point highlights the following differences of opinion between

446 O'Shea I, 22 December 2025, BOS-1 Report of Bruce O'Shea, 22 December 2025, Table 2 at [2.4.5]; [**304.1476**] at [**304.1485**], and Table 3 at [2.4.11]; [**304.1476**] at [**304.1486**] [*O'Shea Report*].

Mr O'Shea and Mr Sibenik, on each of which it will submit that Mr O'Shea's approach is preferable:

393.1 The market valuation approach is appropriate;

393.2 There was an active market for LML, with available trading data from which a valuation can be established;

393.3 There is no foundation for the allegations that:

(a) GNY engaged in market manipulation; and, in turn

(b) The available LML trade price data is "artificial" and does not provide a sound basis for a market valuation;

(c) Trades where an account associated with GNY is on one side and an arm's length third party on the other are appropriate to take into account as market data.

393.4 It is inappropriate to rely on sales of stolen LML token post-Hack as market data for valuation purposes.

394 Permeating every aspect of the assessment of GNY's claim is that only 47 days of trading occurred between LML's ICO and the Hack. A substantial portion of LML trades necessarily involved GNY on one side in that first 47 days because GNY had only just made LML available to the market and therefore held much of the circulating LML tokens.

Standard of proof and nature of valuation of claims

395 An earlier section of these submissions recorded that GNY is required to establish its claim on the balance of probabilities, being the same standard that would apply in an ordinary Court proceeding. But, as also set out earlier, liquidation claim assessments must be undertaken on a pragmatic basis using available, but often imperfect, information.

396 Such considerations take on even greater significance in the context of valuing claims relating to cryptocurrency. The assessment of the value of a cryptocurrency cannot be forensically precise.[447] The

[447] *Fantom Foundation Ltd v Multichain Foundation Ltd* [2024] SGHC 173 at [37].

inherent uncertainty in valuing cryptocurrency is best avoided by focusing on available pre-Hack market data, rather than speculation as to what would or would not have happened to a cryptocurrency. That is the approach that has been taken by Mr O'Shea.

Mr O'Shea's valuation methodology

397 Mr O'Shea is a Chartered Accountant and partner with KordaMentha Forensic in Brisbane, Australia. He has over 20 years' experience in the provision of forensic accounting services, valuations and assessment of loss and damage.[448]

398 Mr O'Shea has extensive experience across a range of industries, including financial services. That includes, most relevantly:[449]

398.1 valuations of cryptocurrency holdings;

398.2 tracing of cryptocurrencies traded through an exchange and consideration of the market prices achieved on the sale of several parcels of that cryptocurrency;

398.3 reviewing and tracing cryptocurrency holdings to quantify compensation payments arising from a cryptocurrency exchange's failure to comply with regulatory requirements;

398.4 assessment of economic loss incurred by a global firm in the financial services industry following an alleged breach of contract.

Valuation approach

399 Mr O'Shea has outlined the commonly used and generally accepted approaches for valuing financial assets:[450]

399.1 *Income approach*: converting estimates for future cash flows to a single current value or a range of current values, being the future net cash flow the financial asset is expected to produce from the time it is held.

---

448 O'Shea Report, 22 December 2025, at [1.1.3]; [**304.1476**] at [**304.1479**].
449 O'Shea I, 22 December 2025, at [4]; [**201.0246**] at [**201.0247**]; O'Shea Report, 22 December 2025, Appendix A, pages 5-6; [**304.1476**] at [**304.1540**].
450 O'Shea Report, 22 December 2025, at [8.3.2]; [**304.1476**] at [**304.1518**].

399.2 *Market approach*: comparing the asset with comparable financial assets. For financial assets that are traded (such as LML tokens), the most appropriate approach may be taking the market price as the most appropriate price.

399.3 *Cost approach*: estimating the costs to replace or reproduce the asset.

400 Mr O'Shea adopted the market approach on the basis that:[451]

400.1 Similar to gold or currency, crypto assets are non-income producing and do not provide the holder with an income stream.

400.2 The value of crypto assets is derived from changes in the market price, based on the economics of demand and supply in the market.

400.3 An active market was present for LML at the time of the hack, as shown in the available data (addressed further below).

400.4 Therefore, a market-based approach is the most appropriate approach since it has an observable market price in an active market.[452]

401 As addressed in more detail below, Mr O'Shea also used the cost approach as a cross-check for his market-based valuation.

LML token market price assessment

402 Mr O'Shea assessed the market price for LML as 0.00003133 BTC per token.[453] That is the weighted average market price in BTC/LML as at 13 January 2019, being the last day of trading that would not have been impacted by the Hack. That figure:

---

451 O'Shea Report, 22 December 2025, at [8.4.1]; [**304.1476**] at [**304.1518**].
452 Mr O'Shea refers to the International Financial Reporting Standards 13 definition of "active market" as "a market in which transactions for the asset… take place within sufficient frequency and volume to provide pricing information on an ongoing basis" (at [9.2.1]); [**304.1476**] at [**304.1520**]. LML tokens were traded on both Cryptopia and BitBay.
453 O'Shea Report, 22 December 2025, at [9.3.4]; [**304.1476**] at [**304.1523**].

402.1 reflected a "conservative approach" and excluded trades from one GNY account to another (which the liquidators have criticised, and which is addressed in more detail below);

402.2 is based on the GT Trading Data provided by and relied on by the liquidators and Mr Sibenik, which Mr O'Shea has been instructed to assume is accurate;[454] and

402.3 does not include the trading data obtained from CoinPaprika, a cryptocurrency research platform, because that data does not allow for GNY-GNY trades to be separated out.

403 Mr O'Shea acknowledged that there were future risks and uncertainties relevant to LML tokens, including that it was an asset in the early stages of its trading and had limited trading history. But it was reasonable to assume that those risks and uncertainties would have been factored into the market price for LML.[455]

Marketability discount

404 Marketability refers to how quickly and easily an asset can be bought or sold in a market.[456] Where markets for an asset have issues with liquidity, a discount for such marketability issues needs to be considered.

405 Mr O'Shea has responsibly assessed that a marketability discount needs to be applied because pre-Hack data from LML trades indicated that the market was not liquid enough to readily sell the relevant quantities of LML tokens being valued. Mr O'Shea had regard to empirical studies which established a reasonable range of 10% to 70% when accounting for marketability of equity assets (e.g. company shares), with an extension to 80% to account for the particular price volatility of crypto assets.[457]

406 Mr O'Shea considered it difficult to assess a precise marketability discount for each of the GNY claims, and accordingly applied a range

---

454 Sibenik I, 31 July 2025, PS1 GrantThornton "Cryptopia LML Trading (GNY)" report, 1 December 2025; [**303.1384**]; Sibenik I, 1 August 2025, at [46]–[47]; [**201.0090**] at [**201.0101**]; O'Shea Report, 22 December 2025, Appendix C (letter of instruction); [**304.1476**] at [**304.1546**].

455 O'Shea Report, 22 December 2025, at [9.2.8]–[9.2.14]; [**304.1476**] at [**304.1520**].

456 O'Shea Report, 22 December 2025, at [9.2.15]; [**304.1476**] at [**304.1521**].

457 O'Shea Report, 22 December 2025, at [9.2.15]–[9.2.20]; [**304.1476**] at [**304.1521**].

(as set out below). Relevantly, he identified a range of factors that would either increase or decrease the marketability discount:[458]

> Factors that would increase the marketability discount include:
>
> i. The LML tokens had only been on the exchanges for 47 days (i.e. a very short window to understand how LML would have gained traction in the market).
>
> ii. The trading volume of the LML token is low based on its 47 days of trading (relative to the quantity of the stolen LML tokens and quantity available for sale to the market).
>
> iii. A portion of the trades during this 47 day period was between GNY parties.
>
> Factors that would decrease the marketability discount include:
>
> i. GNY had passed critical hurdles in bringing LML to the crypto asset market (as shown by its listing on multiple exchanges).
>
> ii. Prior to the Hack trading volumes did appear to be increasing and this growth was interrupted by the Hack (i.e. LML was not provided a chance to succeed).
>
> iii. LML was listed on multiple exchanges and had an observable market price for its tokens.

407 The specific range of marketability discount applied by Mr O'Shea differed for the two different GNY claims, as set out below.

408 GNY addresses in more detail below the appropriate marketability discount to be applied in valuing each claim.

Valuation of GNY's stolen LML tokens claim

409 Mr O'Shea multiplied the assessed market price of a single LML token of 0.00003133 BTC by the amount of stolen LML tokens (15,409,316). That resulted in a base valuation of 482.75 BTC for the stolen LML tokens.

410 Mr O'Shea then applied a discount for marketability issues in the range of 30-50%, being the "*middle range of the equities discount*" referenced above.[459]

---

458 O'Shea Report, 22 December 2025, at [9.2.21]; [**304.1476**] at [**304.1522**].
459 O'Shea Report, 22 December 2025, at [9.2.22(a)]; [**304.1476**] at [**304.1522**].

Lower end of marketability discount range is appropriate

411 GNY submits that the 30% discount, at the lower end of Mr O'Shea's marketability discount range is appropriate, by reference to the factors identified by Mr O'Shea.

LML token not a 'flash in the pan'

412 GNY had not only passed critical hurdles to bring LML to market by listing on multiple exchanges. GNY was not created as "*a 'flash in the pan' token with the intent of making a quick dollar*".[460] A number of features of LML distinguish it from many other crypto assets, which unlike LML are created with the intent to generate value through speculation. Specifically:

412.1 LML ought not be viewed as a standalone token but as part of a wider GNY ecosystem, underpinning development of machine learning models. The LML token (and the separate GNY token) was:[461]

> …intended to be a "utility token" for people to buy and use alongside the AI [GNY was] developing. In substance, people buying the GNY token, and the LML token, would be forward funding further development of [GNY's] AI.

412.2 The LML token reflected GNY's collaboration with Lisk, an existing and much larger community, to whom GNY did extensive outreach.[462]

412.3 In order to get the LML token off the ground and launch its ICO, GNY:

(a) prepared a detailed 'white paper' to provide information to investors about the GNY tokens and the underlying technology;[463] and

(b) obtained approval from the Jersey Financial Services Commission for issuers of initial coin and token offering before launching LML's. That required GNY to meet conditions of governance, investor disclosure and

---

460 [redacted], 19 December 2025, at [38]; [**201.0141**] at [**201.0148**].
461 [redacted], 19 December 2025, at [38]; [**201.0141**] at [**201.0148**].
462 [redacted], 19 December 2025, at [36]; [**201.0141**] at [**201.0148**].
463 [redacted], 19 December 2025, at [38]; [**201.0141**] at [**201.0148**].

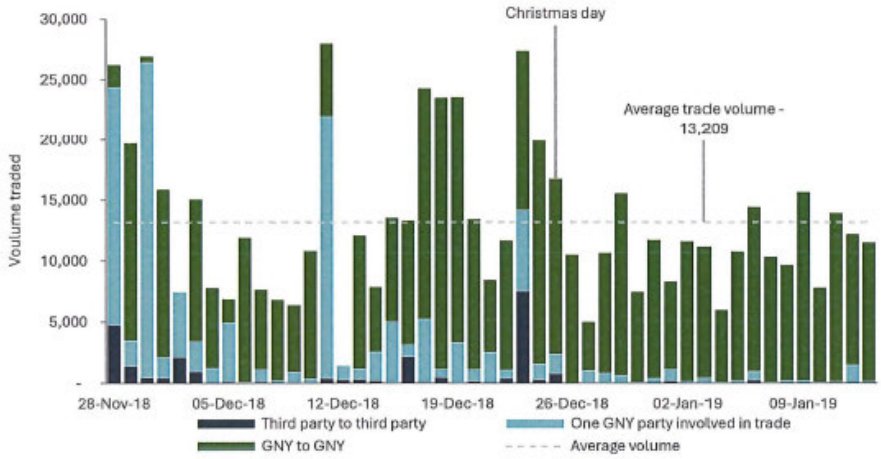
AML/CFT compliance that most token issuers do not meet.[464]

LML upward trend in price and volume apparent in pre-Hack trading

413 While the LML token had only been trading for 47 days prior to the Hack, a sufficient upward trend in volume of LML trades is apparent and justifies application of the lower end of the marketability discount range.

414 Mr O'Shea's breakdown of LML trading volumes over the relevant 47-day period is relevant:

Figure 6: Breakdown of trade volume



Source: KordaMentha; GT Trading Data

415 That breakdown shows:

415.1 An initial high volume of trades in the first days following the LML token launching, before approximately 10 days of quieter trading. From 12 December 2018 to Christmas Day 2018, a general increase in volume of trades can be seen, including in trades involving a third party on at least one side. (The volume of trades which are GNY-GNY only is addressed separately later in these submissions.)

415.2 While a drop in trading volume after Christmas Day 2018 can be observed, GNY submits that is not reflective of a general

[464] [redacted], 19 December 2025, at [47]; [**201.0141**] at [**201.0150**].

trend for LML. The public holiday period post-Christmas is a typically low-trading period.[465] Mr O'Shea identified that in January 2019 "there was a noticeable decrease in crypto asset trading volumes generally".[466]

415.3 The 13 January 2019 Hack prevented the continued growth of the volume of LML trading.

416 GNY submits that the Court can conclude, on the balance of probabilities, that:

416.1 the downward trend in volume between Christmas and the Hack was not reflective of LML's market;

416.2 the pre-Christmas upward trend in trading volume could be reasonably expected to have continued but for the Hack;

416.3 in light of the underlying features of LML and the trends above, it is appropriate to apply the lower end of the marketability discount range.

Valuation of lost market capitalisation claim

417 To value the market capitalisation loss resulting from the Hack as claimed by GNY, Mr O'Shea has assessed the difference in value between:[467]

417.1 the 120 million circulating supply of LML tokens immediately prior to the Hack, on 13 January 2019; and

417.2 the 120 million circulating supply of LML tokens on 30 May 2019, when the hacker stopped the sale of the stolen tokens and the impact of the Hack effectively ceased.

418 As above, Mr O'Shea adopted the market price of 0.00003133 BTC per LML token prior to the Hack, multiplied by 120 million tokens, to get a figure of 3,759.41 BTC.

---

465 [redacted] 19 December 2025, at [52]; [**201.0141**] at [**201.0151**].
466 [redacted] Report, 22 December 2025, at [6.2.14(b)]; [**304.1476**] at [**304.1510**], citing Nasdaq reporting.
467 O'Shea Report, 22 December 2025, at [9.4.7]–[9.4.8]; [**304.1476**] at [**304.1525**].

419 For the value as at 30 May 2019, Mr O'Shea was only able to rely on CoinPaprika data, as the GT Trading Data provided by the liquidators did not go beyond the date of the Hack.[468] That data showed a market price of 0.00000172 BTC per token as at 30 May 2019, and a base figure of 205.81 BTC for the 120 million LML tokens as at 30 May 2019.

420 Subtracting the 30 May figure from the 13 January figure provides a base loss calculation of 3,553.60 BTC (3,759.41 BTC less 205.81 BTC).

421 In response, Mr Sibenik has fairly acknowledged that:

421.1 he cannot say what the market price of LML would have been in May 2019 had the Hack not occurred;[469] and

421.2 it is "reasonable to suggest that the hack may have put downward pressure on the price of LML" from the date of the Hack through to May 2019.[470]

422 The only substantive challenge from Mr Sibenik to Mr O'Shea's assessment of the lost market capitalisation claim is that it is "not rare for a price of a new cryptocurrency token to plummet by 90% in a 6-month period or less".[471] Concluding that LML's price would inevitably have dropped in that fashion regardless of the Hack is speculation, which ought to be avoided.

Lower end of marketability discount range is appropriate

423 Mr O'Shea considered that a 60 to 80% marketability discount was appropriate to apply to the market capitalisation loss.

424 GNY submits, again, that the 60% discount, at the lower end of Mr O'Shea's discount range, is appropriate, for the same reasons as identified above in respect of the stolen tokens claim.

425 Contrary to Mr Sibenik's evidence, it was not "probable" that the LML price would have continued to decline had LML tokens not been

---

468 O'Shea Report, 22 December 2025, at [9.4.11]; [**304.1476**] at [**304.1525**].
469 Sibenik II, 24 February 2026, at [28]; [**201.0257**] at [**201.0265**].
470 Sibenik II, 24 February 2026, at [29]; [**201.0257**] at [**201.0266**].
471 Sibenik II, 24 February 2026, at [28]; [**201.0257**] at [**201.0265**].

stolen in the Hack.[472] Nor is it inevitable that the value of tokens issued by new cryptocurrency projects tend to decline and "'go to zero' sooner or later".

426 Mr Sibenik's attempt to directly compare LML to established cryptocurrencies like Bitcoin and Ethereum does not assist. GNY does not argue that LML was of comparable standing to those established cryptocurrencies at the time of the Hack. But nor was it only a token that someone would buy for speculation. LML was a utility token linked to funding of development of AI machine learning technology. It was always intended to have a long-term functional purpose and accordingly LML tokens were intended to be released and traded gradually by GNY.[473]

Cross check of valuation of lost market capitalisation

427 Mr O'Shea then undertook a "cost approach" valuation as a cross-check for his lost market capitalisation claim valuation.[474] He did so on the basis that LML is a unique asset and its value can be ascertained by quantifying the costs and work required to get a similar token into the market (to the extent possible).[475] The types of relevant costs include financing costs, capital expenditure and/or research and development costs. Mr Sibenik has not criticised Mr O'Shea's cost approach cross-check.

428 Mr O'Shea relied on evidence from [redacted] that 60-65% of the USD 2.95 million invested into GNY (and a prior company, Grey Jean Technologies that was folded into GNY), is attributable to the development of LML.[476] That provided a US dollar range of LML development costs of:

428.1 USD 1.77 million (60% of USD 2.95 million); and

428.2 USD 1.92 million (65% of USD 2.95 million).

429 Mr O'Shea assessed the market capitalisation value of the 120 million LML tokens available to the market using the weighted average price and marketability discount as above, and applying the

---

472 Sibenik I, 1 August 2025 at [29]; [**201.0090**] at [**201.0098**].
473 [redacted] 19 December 2025, at [43]; [**201.0141**] at [**201.0149**].
474 O'Shea Report, 22 December 2025, at [10.1]–[10.4]; [**304.1476**] at [**304.1527**].
475 O'Shea Report, 22 December 2025, at [10.2.2]; [**304.1476**] at [**304.1527**].
476 [redacted] 19 December 2025, at [33]–[39]; [**201.0141**] at [**201.0147**].

60-80% marketability discount range. Converting that into USD for comparison purposes gave a value range between USD 2.75 million and USD 5.5 million. That value range exceeding the cost indicates implicit value in the LML token at the date of the Hack.[477] The cost assessed confirms that Mr O'Shea's market approach calculation is not unreasonable, in addition to being the 'floor' for GNY's claim.

Criticisms of Mr O'Shea's market valuation are unfounded

430 Mr Sibenik's criticisms of Mr O'Shea's market valuation approach are unfounded. There was a genuine, active market for LML tokens providing a sound basis for Mr O'Shea's LML valuation. The allegation that GNY engaged in "market manipulation", and that the pre-Hack LML prices are consequently "artificial", [478] are not warranted. Such serious allegations require compelling evidence.[479]

There was an active market for LML

431 Mr O'Shea has identified three different categories of LML trades from the GT Trading Data provided by the liquidators:[480]

431.1 Trades from one GNY account to another (Mr O'Shea has assumed that the three trading accounts identified by Mr Sibenik as GNY accounts are in fact GNY accounts[481]);

431.2 Trades between a GNY account and a third party (i.e. not GNY) account; and

431.3 Trades between a third party account and a third party account.

432 Mr O'Shea calculated the trading volumes of each of the three categories:[482]

---

477 O'Shea Report, 22 December 2025, at [10.4.6]; [**304.1476**] at [**304.1529**].
478 Sibenik I, 1 August 2025, at [22(b)]; [**201.0090**] at [**201.0096**].
479 *In re H (Minors)(Sexual Abuse: Standard of Proof)* [1996] AC 563 at 586D-H per Lord Nicholls; *Re B (Children) [2008] UKHL 35* at [13] and [15] per Lord Hoffmann; *Z v Dental Complaints Assessment Committee* [2008] NZSC 55, [2009] 1 NZLR 1 at [28].
480 The CoinPaprika Weekly Data does not contain detail of the parties to each trade and so trades in the CoinPaprika Weekly Data cannot be similarly broken down.
481 O'Shea Report, 22 December 2025, at [6.2.5]; [**304.1476**] at [**304.1507**].
482 O'Shea Report, 22 December 2025, at [6.2.6]; [**304.1476**] at [**304.1508**].

Table 10: Trading volumes with GNY Parties and third parties

Trade type	Volume (LML)	Proportion of volume	Number of trades	Proportion of count
GNY Party to GNY Party trades	469,361	51.3%	201	16.2%
Trades between a GNY Party and third party	391,688	42.8%	618	49.8%
Third party to third party trades	54,296	5.9%	422	34.0%
Total	**915,345**	**100.0%**	**1,241**	**100.0%**

Source: KordaMentha; GT Trading Data

433 As set out above, the proportion of trades involving a third party on at least one side is 48.7% by volume, and 83.8% by number of trades.

434 Mr O'Shea and Mr Sibenik are aligned in their views that:

434.1 GNY-GNY trades (i.e. purely internal trades) should be excluded from data used to assess LML market value. The impact of GNY-GNY trades should be excluded to remove any influence of related party trading;[483] and

434.2 Third party-third party trades should be included in assessing LML market value.

435 The parties differ materially about whether GNY-third party trade data can be properly relied on in determining market value.

436 The Liquidators' GT Report (the **GT Report**) seeks to distinguish such trades. The daily trading volumes recorded in GT Report identify "[s]uspicious" trading volumes, comprised only of trades including a GNY account. And they identify an "alternative" volume, being all trades that exclude GNY accounts.

437 In turn, the analysis from the GT Report appears to have been adopted wholly by Mr Sibenik, rather than conducting his own analysis.[484]

438 Mr O'Shea has explained why GNY – third party trades should not be disregarded:[485]

438.1 It is appropriate to include GNY purchases of LML from an arms-length seller in assessing LML market value. The

---

483 O'Shea Report, 22 December 2025, at [7.3.3]–[7.3.5]; [**304.1476**] at [**304.1516**].
484 Sibenik I, 1 August 2025 at [46]–[48]; [**201.0090**] at [**201.0101**].
485 O'Shea Report, 22 December 2025, at [7.2.14]; [**304.1476**] at [**304.1515**].

involvement of a third party in a transaction requires consideration be given to whether the transaction is a market based transaction. On the assumption that the seller is an independent market participant, there is a general assumption in market theory that the seller would only transact at a market price. The approach is particularly affirmed by the fact that the weighted average market price is relatively the same between all of the different trade categories (as above).[486]

438.2 It is also appropriate to include GNY sales of LML to an arms-length purchaser in assessing LML market value.[487] Sales from GNY to arms-length purchaser were an inevitable and unremarkable feature of the early period of trading after GNY launched the LML token.[488]

439 Mr Sibenik's efforts to discount the market theory approach in relation to LML are problematic:[489]

439.1 By properly taking into account trades between GNY and third parties, and not just third party-third party trades, the available market evidence for valuation purposes is materially more significant.

439.2 Under IFRS 13, an active market is a "market in which transactions for the asset...take place with sufficient frequency and volume". What is sufficient is a subjective mater, but needs to be properly contextualised. While the traded LML pre-Hack amounted to only a small portion of circulating LML, the period from the ICO to the Hack was only 47 days long. While that is a relatively brief period of trading compared to other well-known tokens such as Bitcoin, it is nevertheless the best available evidence of LML's market value prior to the Hack. It cannot be right that losses caused by the Hack cannot be assessed because the event of the

---

[486] O'Shea Report, 22 December 2025, at [7.3.6]–[7.3.10]; [**304.1476**] at [**304.1516**].
[487] O'Shea Report, 22 December 2025, at [7.3.11]–[7.3.15]; [**304.1476**] at [**304.1516**].
[488] [redacted], 19 December 2025, at [55]; [**201.0141**] at [**201.0151**].
[489] [redacted] II, 24 February 2026, at [13]–[15]; [**201.0257**] at [**201.0261**].

Hack prevented a greater build-up of LML trading history for valuation purposes.

439.3 It had never been intended that LML would be released at once. Rather, it was intended (and investors were told accordingly) that circulating tokens would be sold in an orderly way over a period of time.[490]

439.4 Suggestions that third parties buying LML did not know about GNY's market-making (addressed below) and that GNY was the counterparty are entirely speculative. A reasonable inference can be drawn that third parties purchasing LML would have known that GNY as the issues would be selling it, in circumstances where the purchases had happened within a month and a half of the ICO.

439.5 It is similarly speculative that "[m]ost people who would have bought LML tokens were effectively gambling".[491] [redacted] has explained (as above) that LML was established as a utility token intended to facilitate AI development, creating a different value proposition to most new tokens.

439.6 To the extent that some LML was purchased speculatively, in the hope of a sell-off after a rapid increase in value, that is no different to the sharemarket. Shares are not impervious to growth in value based on investor sentiment based on "belief about future cash flows and investment risks that is not justified by the facts at hand", as seen with various technological bubbles over time.[492] But even if shares or tokens are being bought speculatively, there is still a market for them and a value that can be assessed.

No evidence of market manipulation

440 Mr Sibenik has, without proper foundation, alleged that much of the trading volume of LML tokens is the result of market manipulation. Specifically, he has alleged that "wash trading" and "circular trading" occurred, being (by his definition) "insiders of the same

---

490 [redacted] 19 December 2025, at [41]–[43]; [**201.0141**] at [**201.0149**].

491 Sibenik II, 24 February 2026, at [14(b)]; [**201.0257**] at [**201.0262**].

492 Malcome Baker and Jeffrey Wurgler "Investor sentiment in the stock market" (2007) 21(2) Journal of Economic Perspectives 129.

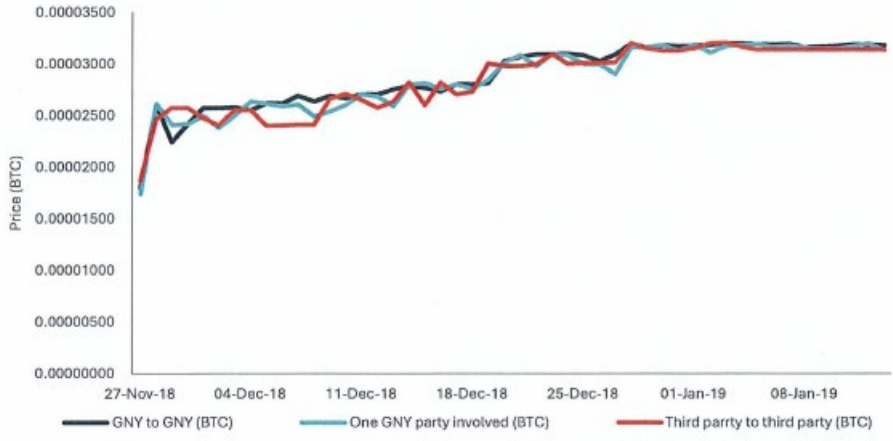
entity artificially boosting volume by making trades amongst themselves to give the appearance of demand and liquidity".[493]

441 The available trading price data (with which Mr Sibenik did not engage) does not bear out that allegation.

442 GNY-GNY trades of LML are closely comparable in price to trades involving third parties taken into account in assessing the market. Mr O'Shea's analysis is clear on this point.

443 The weighted average market price for LML was broadly consistent in the 47-day trading period prior to the Hack, whether or not the trade involved a GNY party:

Figure 7: Weighted average market price for LML across each trade type (BTC pair)



444 The average variation between the average weighted price for each of the trade categories was 1.5%.[494]

445 More specifically, as evidence that GNY-GNY trades did not impact the market price, at different points the GNY-GNY trade price would be less than third party-third party prices (by up to 14.8%). At other times the GNY-GNY trade price would exceed the third party-third party price (by 10.4%). That is visible in Figure 7 above.

446 [redacted] has firmly denied all of the allegations of market manipulation. He has explained the reasons for the GNY-GNY trades at [44]-[61] of his 19 December 2025 affidavit.

---

493 Sibenik I, 1 August 2025, at [45]; [**201.0090**] at [**201.0101**].
494 O'Shea Report, 22 December 2025, at [6.2.18]; [**304.1476**] at [**304.1510**].

447 The internal GNY-GNY trades were market-making, and undertaken by GNY as the issuer at a time when professional market making businesses were far less prevalent.[495] As [redacted] explains:

> In 2018, it was my understanding that it was typical market practice in the crypto-currency world for a token issuer to undertake market-making trades for newly released tokens. Market-making is important to ensure there is sufficient support for the trading of the token, for token purchasers to execute trades on buy or sell side, by ensuring two-sided liquidity (i.e. maintaining both bids and offers for the new token). This is particularly important in the early stages of a token lifecycle when a market is establishing itself and maturing.
>
> Token issuer involvement in token trades helps to stabilise token price in the initial period of a token's release. This can require an issuer to ensure there is a buyer for a token holder wishing to sell at the market price (a form of buy-side market making) or to undertake internal trading to stabilise or close arbitrage prices between different exchanges - as opposed to artificially pumping up prices - for short periods of time. These activities do not result in any monetary gain for the issuer. Rather, they stabilise the newly-created market in order to create an orderly trading environment, which gives the market time and space to grow.

448 Other GNY-GNY trades took place for other reasons, including:[496]

448.1 Test trades to ensure that the exchange was functioning properly;

448.2 Acting as closing arbitrage trades to ensure price alignment across Bitbay and Cryptopia platforms. LML trading became more popular on Bitbay than Cryptopia and arbitrage trades were needed to price rebalance on the quieter exchange;

448.3 Other trades were balancing the LML holdings between the GNY accounts.

449 None of the trades involved the large volumes of trades on an exchange that characterise wash trading. The trades were all executed manually rather than via automatic trading bots and algorithmic rules.[497]

450 In 2018, it was typical practice in crypto-currency for an issuer to undertake such market-making trades.

---

495 [redacted] 19 December 2025, at [50]–[53]; [**201.0141**] at [**201.0150**] and [61]; [**201.0141**] at [**201.0152**].

496 [redacted] 19 December 2025, at [57]; [**201.0141**] at [**201.0152**].

497 [redacted] 19 December 2025, at [58]–[60]; [**201.0141**] at [**201.0152**].

451 Mr Sibenik did not challenge any of [redacted] evidence in his reply. His only observation in response was that he was not aware of GNY's market making being publicly disclosed, and therefore created an unwarranted perception of trading interest. That response ignores [redacted] point that token issuer market making was a standard and well-known feature of crypto-currency in 2018.

452 Mr O'Shea similarly concluded:[498]

> …the involvement of GNY Parties alone does not necessarily give rise to market manipulation. Relevant considerations include:
>
> a. Participation by GNY Parties in the market would have been necessary in the initial trading phase to facilitate the sale of the LML token into the market.
>
> b. The full context, and the extent of, trades between GNY Parties should be assessed before such trades are wholly classified as 'wash trading' or 'suspicious'. The GT Report appears to imply that all trades involving a GNY Party constitute 'wash trading' without considering the underlying reason for those trades.
>
> c. The potential impact on market price also warrants consideration where GNY Parties are involved on one side of the trade, as this may indicate whether any market manipulation occurred. The GT Report does not provide any analysis of the price movements or the composition of the market price in LML.

453 Ultimately the available pricing data as reviewed by Mr O'Shea (with which Mr Sibenik has not engaged) shows no indication of any inflation in price involving GNY trades, and does not support the implication that there was any intentional or artificial inflation.

Alternative valuation approaches used in FTX litigation do not assist

454 Mr Sibenik has identified the existence of an alternative valuation model, put forward to the US Bankruptcy Court in order to assess claims in the bankruptcy of the well-known crypto exchange FTX, following its collapse.[499]

455 The alternative methodology in question does not and cannot assist the Court in the present case. Nor does it serve to displace Mr O'Shea's approach and methodology in any way.

456 At a general level, the US Bankruptcy Court's judgment acknowledges the issue already identified by Mr O'Shea: where a

---

498 O'Shea Report, 22 December 2025, at [5.3.20]; [**304.1476**] at [**304.1503**].
499 Sibenik II, 24 February 2026, at [25]; [**201.0257**] at [**201.0265**].

limited market exists for the parcel of tokens in question, any increase in trading is likely to negatively impact price, and requires a marketability discount.[500] The issue, then is about, the quantum of that marketability discount.

457 The US Bankruptcy Court rejected the use of Professor Howell's "KO Model" (identified by Mr Sibenik)[501] for valuing of parcels of crypto tokens and assessing such a marketability discount.[502] Among other things, the Court found that:

457.1 "the KO Model has not previously been used for the purpose it is being used for here";

457.2 "the purpose of the KO Model is not necessarily to value an asset. Rather, it is to calculate the transaction costs from a decision to take a position in a market of a certain size";

457.3 The discounts to the market price that the KO Model provided for exceeded 100% for several of the digital assets (i.e. the costs of trying to sell the relevant assets would exceed their apparent value).

458 Mr Sibenik has not acknowledged these points in his evidence (although GNY acknowledges the Liquidators' submissions provide some additional context in that regard).[503]

459 Instead, the Liquidators seek to attempt to rely on the US Bankruptcy Court finding that market prices for the relevant tokens may not be a reliable indicator of value because the relevant claimants held 95-99% of the total supply of the tokens.[504]

460 That finding was made in a materially different context to the present case. FTX and its sister cryptocurrency trading firm, Alameda, made available for free float (tokens available for trading in the marketplace) less than 3% of the tokens' maximum supply.

---

500 United States Bankruptcy Court for the District of Delaware *In re FTX Trading et al* Memorandum Opinion and order of June 26, 2024 at 11; [**303.1302**] at [**303.1312**].
501 Sibenik II, 24 February 2026, at [25]; [**201.0257**] at [**201.0265**].
502 United States Bankruptcy Court for the District of Delaware *In re FTX Trading et al* Memorandum Opinion and order of June 26, 2024 at 15; [**303.1302**] at [**303.1316**].
503 Liquidators' Submissions, [8.266].
504 Liquidators' Submissions, [8.269].

Professor Howell referred to commentators suggesting that restricting the free float of the tokens was "a deliberate strategy for FTX and Alameda to inflate the market prices of the at-issue tokens, and in turn inflate the value of FTX's and Alameda's balance sheets".[505] The Court did not make any decision about what FTX and Alameda intended to do by restricting the free float of the tokens.

461 The Court accordingly preferred a valuation model that took into account a lack of marketability due to both:[506]

461.1 contractual "locking" (i.e. a contractual obligation preventing the claimant from selling tokens until a specified contractual date");[507] and

461.2 a lack of liquidity due to an increase in trading volume and/or the circulating supply.

462 In the present case, there was no availability restriction in respect of LML tokens. All 120 million of the circulating supply of LML was able to be bought. GNY held much of the circulating supply of LML at the time of the Hack because the Hack happened only 47 days after the ICO.

463 Given the different contexts, a direct application of the model applied by the US Bankruptcy Court to LML is not appropriate. Nor has Mr Sibenik tried to apply it in his evidence.

464 Moreover, the US Bankruptcy Court's ultimate determination of the marketability discount to be applied is of little assistance:

464.1 The US Bankruptcy Court's judgment indicates that a marketability discount will not necessarily be exactly aligned to the percentage of tokens held by the claimant. This makes sense, as such an approach could only ever be a rough and

---

505 United States Bankruptcy Court for the District of Delaware *In re FTX Trading et al* Memorandum Opinion and order of June 26, 2024 at 23; [**303.1302**] at [**303.1324**].

506 United States Bankruptcy Court for the District of Delaware *In re FTX Trading et al* Memorandum Opinion and order of June 26, 2024 at 22, n 71; [**303.1302**] at [**303.1324**].

507 United States Bankruptcy Court for the District of Delaware *In re FTX Trading et al* Memorandum Opinion and order of June 26, 2024 at 2; [**303.1302**] at [**303.1303**].

ready rule of thumb. While the claimant held 95% of available SRM tokens in that case, the applicable marketability discount was only 18.6%.[508]

464.2 To the extent that Mr Sibenik or the Liquidators wanted to rely on the US Bankruptcy Court's analysis, it would have been necessary to undertake an analysis based on the model adopted by the US Bankruptcy Court, and adduce that analysis into evidence. They have not done so. Nor have they adduced evidence drawing any parallels between the specific nature of the tokens assessed by the US Bankruptcy Court, and LML. At most, Mr Sibenik and the Liquidators have identified that an alternative valuation approach exists without applying it.

465 In the circumstances, Mr O'Shea's approach and evidence is preferable. Mr Sibenik's and the Liquidators' attempt to apply in a generalised fashion valuation models for distinct unrelated tokens is problematic and should be given no or minimal weight. GNY reserves its position on whether Mr Sibenik's evidence is appropriately qualified as expert, or is otherwise substantially helpful within the meaning of s 25 of the Evidence Act 2006.

Stolen LML token sales should be disregarded for valuation purposes

466 Mr Sibenik's evidence is that "the best way to value the stolen LML tokens is to look at what the hacker was able to sell the stolen LML tokens for".[509]

467 The Liquidators' characterisation of that approach as "not an orthodox method of valuation" is a material understatement.[510] Rather, it is illogical, inappropriate and unprincipled as a matter of methodology. As explained by Mr O'Shea (who has properly disregarded stolen token sales in his valuation process):[511]

---

508 For two other tokens the US Bankruptcy Court applied marketability discounts of 100% and 99.9% respectively to tokens of which 99% and 97% were held by the claimant: United States Bankruptcy Court for the District of Delaware *In re FTX Trading et al* Memorandum Opinion and order of June 26, 2024 at 22; [**303.1302**] at [**303.1323**].

509 Sibenik I, 1 August 2025, at [51]; [**201.0090**] at [**201.0102**].

510 Liquidators' Submissions, [8.306].

511 O'Shea Report, 22 December 2025, at [7.2.4]; [**304.1476**] at [**304.1514**].

> I do not consider it appropriate to factor in any aspect of the sale of the stolen LML tokens or failure to sell all of the stolen LML tokens for several key reasons, being:
>
> a. Valuation theory adopts a perspective that it is not appropriate to use hindsight in undertaking an assessment of value. In assessing the value of the coins that were hacked, the Hack in itself is an intervening event that would impact the value of the coins and therefore any events that have occurred after the date of the hack should not be considered in a valuation.
>
> b. I would generally consider it inappropriate to use the trading or sale of stolen assets as a basis for a market price. The LML tokens in general would be imputed with the wider market knowledge of the Hack. This is even more critical to the LML tokens when compared to hacks of other more established tokens as it had only been trading for a very short time and was not widely established in the market.
>
> c. I further would not consider the actions of the hackers to reflect an active and logical market participant. I would not consider it within my area of expertise to guess as to why a hacker would take certain actions or act in a certain way when realising stolen assets.

468 The hacker's sales cannot be reflective of the market in circumstances where:

468.1 Approximately 1.6 million of the 15.4 million of the stolen LML tokens were ultimately sold.[512]

468.2 All of the LML tokens sold by the hacker (approximately 1.6 million of the total 15.4 million LML tokens stolen) were sold on Etherdelta.[513] Etherdelta was a decentralised exchange, which allowed users to transact in an anonymised way (compared to centralised exchanges which are required to collect and store users' personal information and identification, for compliance with regulatory and AML requirements). Etherdelta's front-end operation had been shuttered in the course of 2018 after the SEC had taken enforcement action against Etherdelta's founders for operating an unregistered securities exchange.[514] Because, however, decentralised exchanges can be set-up to operate autonomously (i.e. without front-end operations), Etherdelta nevertheless continued to be used. Contemporary articles noted that EtherDelta was actively used by hackers and

---

512 Sibenik I, 1 August 2025, at [52]–[54]; [**201.0090**] at [**201.0102**].
513 Sibenik I, 1 August 2025, at [54]; [**201.0090**] at [**201.0103**].
514 Westlaw Practical Law Corporate & Securities, 14 November 2018: *EtherDelta: SEC Issues First-Ever Enforcement Action Against Digital Asset Trading Platform by Practical Law Corporate & Securities.*

criminals to launder proceeds from cryptocurrency thefts from the Cryptopia hack in January 2019.[515]

468.3 The 72 trades took place between 15 March 2019 and 29 May 2019. That period started approximately two months after the Hack. By that point the Hack (and the theft of LML tokens) had become widespread public knowledge.[516] Tokens which are known to be stolen (or at least potentially be stolen) are naturally devalued in any market, and do not reflect the market price but for the Hack.

468.4 It can be readily inferred that the hacker sold the LML tokens in an effort to realise ill-gotten gains at speed, rather than to achieve the best price obtainable in the market.

468.5 The heavily reduced price obtained by the hacker for the stolen LML tokens reflects the loss of value attributable to the Hack, rather than the true market value but for the Hack.

469 Mr Sibenik goes on to speculate that the other 13.8 million of LML tokens were not sold because of a lack of liquidity or inability to obtain a good price.[517] On that basis, Mr Sibenik disregarded those tokens entirely from the stolen tokens claim assessment. Again, what could or could not be sold post-Hack is irrelevant, and there is no basis to suggest the same circumstances would have arisen prior to the Hack. To the extent that any marketability discount has to be applied to the total parcel of 15.4 million stolen LML tokens, Mr O'Shea has done so already.

Token swap was not a realistically available option

470 Mr Sibenik has suggested that GNY could and should have performed a "token swap" to mitigate losses suffered in the Cryptopia hack. The "token swap" Mr Sibenik proposed would see new tokens "issued and designated as LML tokens going forward, and old LML tokens would be deprecated".

---

515 See, for example, https://peckshield.medium.com/follow-the-money-tracking-the-asset-movements-of-cryptopia-hack-1485ff202985 and https://coingeek.com/cryptopia-hackers-liquidated-stolen-crypto-mostly-through-etherdelta/.

516 See for example: https://itbrief.co.nz/story/police-making-progress-into-cryptopia-breach.

517 Sibenik I, 1 August 2025, at [55]; [**201.0090**] at [**201.0103**].

471 The Liquidators bear the onus of proving any failure to mitigate. The question is one of fact: whether GNY failed to take reasonable steps in all the circumstances to mitigate the harm suffered.[518]

472 In assessing what is reasonable, GNY's conduct post hack need not be "weighed in nice scales".[519] GNY was not required to:

472.1 adopt measures that could be viewed as view as less burdensome to Cryptopia;[520]

472.2 go to extreme lengths or to pursue every available option;[521] and

472.3 take steps in mitigation that would cause commercial harm or prejudice its commercial reputation.[522]

473 The statement from Lord MacMillan in *Banco de Portugal v Waterlow* is pertinent:[523]

> … it is often easy after an emergency has passed to criticise the steps which have been taken to meet it, but such criticism does not come well from those who have themselves created the emergency. The law is satisfied if the party placed in a difficult situation by reason of the breach of a duty owed to him has acted reasonably in the adoption of remedial measures and he will not be held disentitled to recover the cost of such measures merely because the party in breach can suggest that other measures less burdensome to him might have been taken.

474 [redacted] has addressed in detail in his evidence why a token swap was theoretically possible, but would not have made good sense for GNY:[524]

474.1 performing a token swap so soon after the LML launch, in the midst of market confusion and uncertainty following the Hack, "would have risked destroying *confidence* in our project as a

---

518 *British Westinghouse Electric & Mfg Co Ltd v Underground Electric Railways Co of London Ltd (No 2)* [1912] AC 673 (HL) at 689.

519 *Sullivan v Darkin* [1986] 1 NZLR 214 (CA) at 223.

520 *Banco de Portugal v Waterlow & Sons Ltd* [1932] AC 452 (HL) at 506.

521 *Lesters Leather & Skin Co v Home & Overseas Brokers* (1948) 64 TLR 569 (CA) at 570.

522 *Bradfields Ltd v Brookwater Investments Ltd* [2020] NZHC 935 at [230].

523 *Banco de Portugal v Waterlow* (1932) AC 452 at 506, cited in *Bradfields Ltd v Brookwater Investments Ltd* [2020] NZHC 935 at [229].

524 [redacted] 19 December 2025, at [5]–[32]; [**201.0141**] at [**201.0142**].

whole", and "would have been destructive in terms of value and *reputation*";[525]

474.2 contrary to Mr Sibenik's assertion GNY was not already planning a token swap following the Hack;[526] and

474.3 there was a small window after the Hack when a token swap may have been theoretically feasible once all of the stolen LML tokens were able to be isolated to a specific wallet. However, even if it had been desirable for GNY to undertake the swap (and [redacted] has explained it was not), the swap could not be undertaken without the co-operation of Bitbay, on which LML was listed. Cryptopia did not communicate with Bitbay to provide it with necessary information, as it had been asked to do.[527]

475 Had Cryptopia taken steps to recover stolen LML tokens from other exchanges and implement rebates for stolen LML, there would have been no need for a token swap.[528] But Cryptopia did not take such steps despite being prompted to repeatedly.[529]

476 In his reply evidence, Mr Sibenik's only comment on the token swap was to assert that the administrative costs of the swap would be USD 5,000-30,000. [redacted] evidence about why the token swap was not a viable option for GNY stands unchallenged.

477 A token swap was not a reasonable step that GNY could have been required to take in mitigation. Mr Sibenik's suggestion is an unrealistic hindsight criticism of GNY's response to an emergency of Cryptopia's making. Similarly, the Liquidators' suggestion in submissions that GNY, a Hack victim and trust beneficiary, should have variously sued Bitbay (presumably in addition to Cryptopia), or implemented blacklisting functionality, or undertaken an immediate token swap straight after the Hack occurred go well beyond any

525 [redacted] 19 December 2025, at [8]–[9]; [**201.0141**] at [**201.0142**].
526 19 December 2025, at [10]–[11]; [**201.0141**] at [**201.0143**].
527 19 December 2025, at [12]–[15]; [**201.0141**] at [**201.0143**].
528 19 December 2025, at [18]; [**201.0141**] at [**201.0145**].
529 19 December 2025, at [20]–[30]; [**201.0141**] at [**201.0145**].

realistic approach to mitigation, and could not reasonably be characterised as matters of causation.[530]

Bitbay trading data not available

478 The Liquidators' have unjustifiably criticised GNY for "fail[ing] to provide any records of trading of the LML token on Bitbay".[531] In particular they criticise GNY for not keeping such data in light of GNY filing proceedings against Cryptopia in 2018.[532] There is no basis for any such criticism. The Liquidators' suggestion that, in 2025, GNY should have continue to hold such data because it was potentially (but not obviously) discoverable in a proceeding that was permanently stayed in May 2019 is not a realistic or reasonable suggestion.

479 The Liquidators did not seek any Bitbay trading data for LML at the time prior to provisionally accepting GNY's claim in 2020. It was not until 28 March 2025 (almost five years later) that the Liquidators for the first time requested such Bitbay trading data.[533] By letter dated 3 April 2025, GNY (via counsel) explained that "[f]ollowing withdrawal of the LML token in 2023 GNY no longer has access to Bitbay's trading data: LML is no longer listed on that exchange and GNY's account has been made inactive".[534]

480 The Liquidators requested the data in March 2025 in connection with their unsubstantiated allegation of market manipulation (addressed earlier). That is not an allegation GNY could have foreseen before it was made.

481 GNY provided the Liquidators with information with all available information it could. It provided copies of its deposits and withdrawals from the time LML was listed on Bitbay until June 2021, when GNY stopped maintaining those records.[535] It had also previously, on 6 October 2020, provided market showing trade volume and price for LML, from the date that LML was first listed to

---

530 Liquidators' Submissions, [8.340].

531 Liquidators' Submissions, [8.297].

532 Liquidators' Submissions, [8.22(a)] and [8.297].

533 Email from Liquidators' counsel to GNY's counsel re request for information regarding GNY, 28 March 2025; [**303.1403**].

534 Letter from GNY's counsel to Liquidators' counsel re request for information regarding GNY, 2 April 2025 at [3]; [**303.1404**].

535 Letter from GNY's counsel to Liquidators' counsel re request for information regarding GNY, 2 April 2025 at [4]; [**303.1404**].

September 2020.[536] At no point has GNY sought to withhold any information.

Conclusion on valuation of GNY's claim

482 GNY submits that the Court should determine that GNY's claims are valued as follows, based on Mr O'Shea's orthodox market valuation approach:

482.1 337.92 BTC for the stolen LML tokens claim; and

482.2 1,421.44 BTC for the lost market capitalisation claim.

536 Letter from GNY's counsel to Liquidators' counsel re request for information regarding GNY, 6 October 2020 at [4]–[6]; [**303.1042**].

SECTION 10: DISTRIBUTION OF SURPLUS TRUST ASSETS

Overview

483 The Liquidators' 12 June 2025 report states that "at this stage, it is unclear if there will be any funds available to pay out the unsecured creditors", which total $22.263m (not including GNY's claim).[537] At the same time, the Liquidators confirm that there will be significant unclaimed assets remaining in the Trusts after the distribution process is complete.[538]

484 Those unclaimed assets are held on trust for account holders. Without further order of this Court, they are not available for distribution to meet Hack victim or creditor claims. If that remains the case, the end result of the liquidation will be that:

484.1 claiming account holders' claims in respect of their positive holdings at the date of liquidation will generally be met in full; but

484.2 creditors and Hack victims will be left unpaid, despite a significant surplus of unclaimed trust assets.

485 Against that background, the Court is presented with two alternative pathways:

485.1 the Liquidators' proposal that the Court should order the sale of trust assets to convert into fiat currency, for transfer to the New Zealand Crown; or

485.2 GNY's proposal, that the Court should make unclaimed assets available to meet the claims Cryptopia's creditors, including Hack victims.

486 Neither of these options can be achieved by a legally straightforward method.

487 As the Liquidators correctly acknowledge, their proposal will require the Court to enable a step outside the terms of the Trusts: e.g. to

---

537 Ruscoe I, 31 July 2025, DIR1-56, Thirteenth liquidators' report on the state of affairs of Cryptopia Limited (in Liquidation), dated 12 June 2025; [**303.1421**].

538 Liquidators' Submissions, [10.1], referring to Ruscoe III, 23 April 2026, at [8]; [**401.0026**] at [**401.0028**].

confer on the trustee a power of sale either under the Court's inherent jurisdiction or pursuant to s 130 of the TA. That power is not impliedly within the necessary scope of a trustee's powers. It is directly inconsistent with the fundamental purpose of the Trusts.[539]

488 The Liquidators ask the Court to confer that power on the trustee with the intent of facilitating the payment of unclaimed trust assets to the Crown – notwithstanding ample authority that payment of unclaimed trust assets to the Crown is an unsatisfactory step of last resort, to be avoided if there is any viable alternative. And notwithstanding the practical reality that trust beneficiaries have had years to seek the return of trust assets, but have not done so, and are increasingly unlikely to ever do so. The actual end result of this pathway will be the enrichment of the Crown.

489 There is a better alternative. The Court can (and should) make orders enabling the unclaimed assets to be used to meet creditor and Hack victim claims, particularly in the absence of company funds and assets that would otherwise be available for that purpose. GNY's position is that unclaimed assets:

489.1 should be made available for account holder Hack victims, and general trade creditors. There is in principle no difference between the two for the purposes of distribution; and

489.2 Hack victims should be compensated to the amount of their entitlement, just like any other creditor. While the Liquidators have not provided any evidence of likely Hack victim numbers or claim amounts, it is likely that the majority of Hack victims will have a claim to the value of their account holdings. Only listing entities like GNY may have broader damages claims.

490 No one – account holders (eligible or non-eligible), Hack victims or creditors – should receive more than their entitlements. Rather, available assets should be made available to meet those entitlements on a fair and principled basis.

---

539 Liquidators' submissions, [10.25] and [10.28].

491 There are a range of avenues available to the Court by which it can achieve that practical outcome, in a manner consistent with established trust law. The Court could:

491.1 make distribution orders in the interests of justice and finality pursuant to the Court's inherent jurisdiction; and / or

491.2 vary or resettle, or terminate, the Trusts;[540] and / or

491.3 make a declaration of the Trusts' expiry and vesting of assets in Cryptopia;[541] and / or

491.4 require the Crown to make payment towards outstanding claims of creditors or Hack victims in the event the Court requires the liquidators to transfer surplus trust assets to the Crown.[542]

492 The Court's jurisdiction to make orders of this kind is wide in scope.[543] In addition to powers under the TA, it has an inherent jurisdiction to enable practical difficulties to be overcome in the administration of trusts.[544] The Court's exercise of its inherent jurisdiction to release unclaimed trust assets to meet creditor and Hack victim claims is both appropriate and necessary in this case.

493 Importantly, the rationales provided by the Liquidators in support of their proposal to the transfer of the unclaimed assets to the Crown (such as emergency and necessity) are not exclusive to that pathway. The same reasons apply with equal force to making unclaimed assets available to creditors and Hack victims.

494 Stepping back, both pathways are somewhat unorthodox – but both are legally available to the Court. The Court's choice is ultimately discretionary. One path leads to an outcome which would very likely enrich the Crown with little benefit to account holders, while

---

540 Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025 at [3.18]; [**101.0016**] at [**101.0024**].

541 Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025 at [3.19]; [**101.0016**] at [**101.0025**].

542 Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025 at [3.20]; [**101.0016**] at [**101.0025**].

543 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [22].

544 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [22].

leaving creditors, including Hack victims, unsatisfied. The alternative outcome would satisfy claims from creditors or Hack victims in circumstances where there are available trust assets which are unclaimed from account holders who have not participated in a process ongoing for seven years, despite significant efforts taken to engage those account holders.[545]

The Trusts

495 Before turning to the available pathways, it is important to recognise that the nature of the Trusts is essential context for the Court's jurisdiction, and its decisions on how to deal with unclaimed Trust assets.

496 As the Liquidators appropriately acknowledge in their submissions, the nature of the Trusts in this case is that they are post-hoc and Court-ordered in the Trust Decision[546] with the explicit purpose of allowing for the mechanics of distribution of trust property.

503 This observation is true of a key feature of the Trusts: their scope. In the Trust Decision, Gendall J determined that Cryptopia held cryptocurrencies on express trusts for the benefit of account holders, and that a separate trust existed in respect of *each cryptocurrency*.[547] In effect, this means all account holders for one particular currency (Bitcoin, Doge, Ethereum, for example) are beneficiaries under that one Trust, but not as between Trusts.[548] A trust came into existence for each of the cryptocurrencies as soon as Cryptopia came each time to hold a new cryptocurrency for account holders.[549] Cryptopia itself is a beneficiary of some of those Trusts.[550] Hack victims who held Ethereum and ERC-20 tokens find themselves the beneficiaries of Trusts with no assets.

497 The scope of the Trusts is not apparent from the Terms & Conditions which advise account holders that coins are held on trust. Nor does

---

545 Liquidators' Submissions, [10.45].
546 Liquidators' Submissions, [3.7]. This is the case, notwithstanding that the legal effect of the Court's finding is, in practical terms, retrospective, because the Trusts were found to have been created at the point in time at which a currency was traded on the exchange.
547 *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728, [2020] 2 NZLR 809 per Gendall J at [187]; [**401.0365**] at [**401.0429**].
548 At [183].
549 At [155].
550 At [146].

this finding of scope reflect any identifiable settlor intention or account holder expectation. Rather, this finding in the Trust Decision appears to be based on Cryptopia's internal SQL database,[551] reinforced by the Court's assessment of overall "circumstances", made in the absence of available evidence of settlors' understanding or intention, and in a context where there was a general lack of documentation of trustee stewardship.[552]

498 There was no trust deed to construe, nor factual matrix of settlor intentions regarding the scope of the Trusts, nor material evidence of prior trustee stewardship and administration. As the Liquidators have said, neither Cryptopia nor account holders likely conducted themselves with a trustee / beneficiary relationship in mind.[553]

499 It follows from this context that, very unusually, the trustee's conscious discharge of its trustee obligations has primarily (if not exclusively) been in the course of its long insolvency and through the actions of the Liquidators. At all times the discharge of those duties has been undertaken under the supervision of the Court, and pursuant to detailed directions issued by the Court. Primarily, those steps have been directed to the return of assets to those account holders who happen to be beneficiaries of solvent trusts.

504 Because of the post-hoc nature of the Trusts, there are inevitably significant gaps in relation to how the Trusts should operate. In the Trust Decision, the Court found it was not necessary nor practicable to list all the terms that might govern the Trusts in question,[554] save for finding Cryptopia was and is simply acting as a bare trustee.

505 There is therefore significant latitude for the Court to "fill in the gaps" to ensure the due supervision of, and proper intervention in, the administration of these particular Trusts.[555] This can be done

---

551 *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728, [2020] 2 NZLR 809 per Gendall J at [151-157]; [**401.0365**] at [**401.0419**] – [**401.0420**].

552 *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728, [2020] 2 NZLR 809 per Gendall J at [151] – [166], discussing certainty of intention; [**401.0365**] at [**401.0419**] – [**401.0423**].

553 Liquidators' Submissions, [3.7].

554 *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 728, [2020] 2 NZLR 809 at [195]; [**401.0365**] at [**401.0430**].

555 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [45.2.2]: "the inherent jurisdiction should be regarded as being as wide as is necessary to ensure the due supervision of, and proper intervention in, the administration of trusts, with statutory provisions understood, so far as possible, as elucidating in whole or in part that jurisdiction. Only where

through the inherent jurisdiction, or application of discretionary powers in the TA.

506 The inherent jurisdiction of a Court to supervise and intervene in the administration of a trust is not affected by the TA, except to the extent the TA provides otherwise.[556] In exercising its inherent jurisdiction, a court is to have regard to the purpose and principles of the TA.[557] The relevant principles set out in the Act provide that a trust should be administered in a way that is consistent with its terms and objectives; and avoids unnecessary cost and complexity.[558]

507 Recourse to powers under the inherent jurisdiction or TA is also appropriate and necessary to the extent Gendall J's finding – that each different cryptocurrency was held on different trust, cannot be commingled or accessed by other beneficiaries, even if their trust was exhausted – had a mechanical or administrative dimension to enable appropriate distribution. Such mechanics, however, should not result in a perverse outcome of disclaiming vast amounts of unclaimed assets to the Crown when Hack victims and creditors remain unpaid.

Distribution orders

Distribution Judgment

508 In 2023, the Liquidators filed an application for directions as to the distribution of the trust assets (the **Distribution Application**).[559] By the time of the Distribution Application, the Liquidators had launched their claims portal to identify beneficiaries, verify their identities, and verify their entitlements (of which, at that time, 13.87% of total users had registered, 61.12% of account holders

---

there is a clear and deliberate interference in the width of the inherent jurisdiction by a statutory provision should a Court conclude there is no room for it. So, where statutory processes only give partial effect to the inherent jurisdiction, a court should not refrain from applying the inherent jurisdiction in order to address matters outside the scope of the statutory process, unless it is persuaded that the limited statutory scope was intended as a deliberate restriction of the inherent jurisdiction."

556 Trusts Act 2019, s 8(1).
557 Trusts Act 2019, s 8(2).
558 Trusts Act 2019, s 4.
559 Originating application for directions in respect of distribution of cryptocurrencies, 31 July 2023; [**401.0439**].

had completed identity verification, and 81.02% had completed balance acceptance).[560]

509 In his judgment of 1 March 2024 (**Distribution Judgment**), Palmer J made orders approving the directions sought by Liquidators for the distribution of the cryptocurrencies held on trust by Cryptopia to account holders and the application of trust administration (the **Distribution Orders**).[561]

510 The Distribution Orders affect the interests of account holders who did not register their claims prior to the Soft Cut-off Date (31 March 2025) and Final Cut-off Date (originally 31 December 2024, varied by subsequent orders to be 30 September 2025),[562] and account holders who participated but did not complete the process by the Final Cut-off Date.[563] The Distribution Orders permitted the Liquidators to:

510.1 distribute cryptocurrency on the basis that non-claiming account holders who have not registered their claims by the Soft Cut-off or Final Cut-off Date are "not in existence, even when that account holder is shown in Cryptopia's records as having a beneficial entitlement";[564] and

510.2 treat non-claiming account holders who have participated but had not completed the process by the Final Cut-off Date as having "abandoned their claim with consequence loss of entitlement to receive a distribution".[565]

511 The Court-ordered Final Cut-off Date has passed. Mr Ruscoe reported that as at 31 July 2025, the Liquidators had distributed over NZD $450 million worth of BTC (valued at the respective dates of distribution) and DOGE in three tranches, with the first made shortly before Christmas 2024.[566]

---

560 *Ruscoe v Houchens* [2024] NZHC 419 at [2] and [28]; [**401.0503**] at [**401.0505**] and [**401.0514**].
561 *Ruscoe v Houchens* [2024] NZHC 419 at [58]; [**401.0503**] at [**401.0526**].
562 Sealed Order (Varied Order for Distribution), dated 23 April 2025; [**401.0558**].
563 *Ruscoe v Houchens* [2024] NZHC 419 at [58]: Order 2.2 and 2.5. [**401.0503**] at [**401.0526**].
564 *Ruscoe v Houchens* [2024] NZHC 419 at [58]: Order 2.2; [**401.0503**] at [**401.0526**].
565 *Ruscoe v Houchens* [2024] NZHC 419 at [58]: Order 2.5; [**401.0503**] at [**401.0526**].
566 Ruscoe I, 31 July 2025, at [18]; [**201.0023**] at [**201.0028**].

Abandoned claims

512 In making the Distribution Orders, Palmer J set out the authority for *Re Benjamin* orders, noted its partial codification in s 136 of the TA, and the authority of *Re Instant Cash Loans*.[567]

513 The Court did not explicitly make clear which aspect of its jurisdiction it relied upon. There are distinctions between the original *Re Benjamin* jurisdiction, the development of that jurisdiction, the partial codification of *Re Benjamin* under s 136 of the TA, and the Court's inherent jurisdiction in respect of situations that are similar to, but which do not neatly fit the *Re Benjamin* jurisdiction.

514 *Re Benjamin* orders are made by the Court in exercise of its inherent jurisdiction to supervise trusts.[568] They allow a trustee to make a distribution on the basis of particular facts or footing, where the true facts or footing are impossible or impracticable to ascertain.[569] A typical situation subject to a *Re Benjamin* order involves a trustee faced with a practical difficulty of establishing the existence of possible beneficiaries or other claimants. The Court in that instance will give a direction to the trustees enabling them to distribute the trust property on the assumption of fact that there is no such beneficiary or claimant.[570]

515 The *Re Benjamin* jurisdiction has since expanded beyond enabling trustees to distribute the trust on a particular factual basis.[571] In addition, it has been accepted that the Court has jurisdiction to authorise trustees to distribute without regard to a claim.[572] It has also been accepted the Court's power extends to authorising

---

567 *Ruscoe v Houchens* [2024] NZHC 419 at [25]–[26]; [**401.0503**] at [**401.0513**].
568 *Re Triple A Trustees Ltd* [2020] NZHC 1314 at [13].
569 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [45.3]; *Re Benjamin* [1902] 1 Ch 723: In *Re Benjamin,* Joyce J found that, for the purposes of trust distribution, Mr Benjamin was presumed dead because he could not be found.
570 *In re MF Global UK Ltd (No 3)* [2013] EWHC 1655 (Ch) at [26].
571 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [45.3].
572 *Moss v Integro Trust (BVI) Ltd* (1997/8) 1 OFLR 427 (BVI); *Sinel Trust Ltd v Rothfield Investments Ltd* [2003] JCA 048; and *Fiduciary Trust Ltd v None Named* (13 April 2018, Gibraltar Supreme Court).

trustees to act on a legal opinion as to whether certain assets are or are not held on trust and, if so, what the beneficial interests are.[573]

516 Section 136 re-enacts s 76 of the now-repealed Trustee Act 1956 and partly codifies the common law authority for *Re Benjamin* by permitting the Court to allow the trustee to distribute a missing beneficiary's share; as if a beneficiary "does not exist, never existed, or has died before a date or an event specified".[574]

517 The *Re Benjamin* orders do not vary or destroy beneficial interests: they enable trustees to distribute trust property according to practical probabilities.[575] Any person beneficially entitled may still make a claim for the trust property and may follow the trust property.[576]

518 The English High Court has expanded this aspect of the inherent jurisdiction to allow distributions of shares of beneficiaries who are known to exist – but who have not engaged or properly engaged with a distribution process. In *Re MF Global* the Court approved a distribution procedure allowing distributions on the basis that only those who lodged claims by a specified date would participate, and rejected claims would be disregarded unless the claimant appealed.[577] The Court acknowledged:[578]

> The fact that the proposed order does not in this respect neatly fit within the *Re Benjamin* line of cases does not mean that it falls outside the proper scope of the inherent jurisdiction of the court.

519 The Court's inherent jurisdiction in these instances is wide in scope.[579] Its purpose is to enable practical difficulties to be

---

573 Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [39-036]; Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [45.3].

574 Section 136(1)(a), or under s 136(1)(b): if, because of the order, it is not possible or practicable to determine whether any condition or requirement affecting a beneficial interest in the property or any part of it has been complied with or fulfilled, as if that condition or requirement had been or had not been complied with or fulfilled.

575 *In re Greens Will Trust* [1985] 3 All ER 455 at 462; *In re MF Global UK Ltd (No 3)* [2013] EWHC 1655 (Ch) at [26]; Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [39-031].

576 Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [39-031].

577 *In re MF Global UK Ltd* (No 3) [2013] EWHC 1655 (Ch) at [21].

578 *In re MF Global UK Ltd* (No 3) [2013] EWHC 1655 (Ch) at [30].

579 *Re Instant Cash Loans Ltd* [2021] EWHC 1164 (Ch) at [22].

overcome in the administration of the trust[580] and give practical effect to a trust: [581]

> The purpose of the court's inherent jurisdiction is to enable practical effect to be given to a trust … The administrators' proposals … properly balance both the interests of established clients to a timely return of their money and the interests of persons with serious but unresolved claims to be treated as clients.

520 The aspect of the order in *Re MF Global* which did not neatly fit the *Re Benjamin* jurisdiction was that the rejected claimants did exist in fact, but the proposed order would allow distributions on a presumption that "only good or potentially good claims are those which have been agreed and those whose rejection is the subject of an appeal to the court".[582]

521 Similarly, the Court in *Re MF Global* recognised the order sought did not purport to vary the beneficial interests of the clients and provided the exclusion of any claimant from distribution is without prejudice to their right to participate in any subsequent distribution from the client money trust - and was without prejudice to any available remedy such as tracing.[583]

522 In *Re Instant Cash Loans* recognised the scope of the Court's inherent jurisdiction was wider again. The Court permitted a trustee to proceed on the basis that beneficiaries who had started the claims process, but not completed it by providing bank account details, after further payment attempts were made by trustees, had in fact "abandoned their claim".[584]

523 Against that background, in the Distribution Judgment, the Court appears to have invoked the jurisdiction recognised in *Re Benjamin*, *and* the expanded jurisdiction recognised in *Re Instant Cash Loans*:

523.1 allowing the liquidators to treat those who have not engaged or who partially engaged with the claims process as having "abandoned their claims";[585] and

---

580 *Re Instant Cash Loans Ltd* [2021] EWHC 1164 (Ch) at [22].
581 *In re MF Global UK Ltd* (No 3) [2013] EWHC 1655 (Ch) at [32].
582 *In re MF Global UK Ltd* (No 3) [2013] EWHC 1655 (Ch) at [29].
583 *In re MF Global UK Ltd (No 3)* [2013] EWHC 1655 (Ch) at [21].
584 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [29].
585 *Ruscoe v Houchens* [2024] NZHC 419 at [26]; [**401.0503**] at [**401.0514**]. Applying *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [29].

523.2 allowing the liquidators to distribute trust property as if the non-claiming account holders, as a class of potential beneficiaries "does not exist", reflecting the wording of s 136(1)(a) of the TA.[586]

Approach to abandoned claims

524 The Distribution Orders were made after the claims portal had opened, but before the claims process had finished. The Court is being asked to confirm the treatment of unclaimed assets now that the Final Cut-off Date has passed.

525 Notwithstanding its notice of opposition, GNY accepts that it is unlikely that the Court has a sufficient evidentiary or jurisprudential basis on which to conclude that non-claiming account holder beneficial interests have been extinguished to this point as a matter of *law*.[587] However, as a matter of fact, non-eligible account holders can be said to have abandoned their unclaimed assets. This factual reality underpins the orders permitting the trustee to lawfully conduct itself on the basis that abandonment has occurred, and those legal claims are no longer in existence.

526 The fact of non-claiming account holders' subsisting legal interest is not a barrier to final distributions of available trust assets on a basis other than in accordance with the strict terms of the trust.

527 One available course is for the Court to invoke its inherent jurisdiction in a *Benjamin*-like situation to distribute unclaimed funds without explicitly extinguishing beneficiary rights, following the English High Court's approach in *Re Instant Cash Loans.*[588]

528 Orders made by the English High Court in *Re Instant Cash Loans* dealt with the final distribution of unclaimed trust assets, after it

---

586 Trusts Act 2019, s 136(1)(a): "as if a potential beneficiary or a class of potential beneficiaries does not exist or never existed or has died before a date or an event specified".

587 Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025, [3.17]; [**101.0016**] at [**101.0023**].

588 *Re Instant Cash Loans* [2021] EWHC 1164.

was established that beneficiaries had not engaged with the process and therefore had abandoned their claims.[589]

529 The present circumstances are comparable to those in *Re Instant Cash Loans.* In that case, a company in voluntary liquidation sought the Court's assistance in relation to the distribution of funds held on trust for certain of its creditors as beneficiaries under the terms of a scheme of arrangement. The scheme required payments to be made to the beneficiaries via bank transfer. But a significant number of beneficiaries (about 19.5% by value, £59 million in gross claim value) had not supplied the company with the necessary bank account details which prevented the company from making the payments.

530 Because the beneficiaries had not provided their bank details and seemingly displayed a lack of intention to claim their entitlement, "they could be regarded by the court and the Company as having decided to abandon their claim". The Court was referred to four factual matters in support of this view:[590]

530.1 the relevant scheme sought to pay creditors' claims after costs;

530.2 there had been "an extensive communications exercise" to encourage creditors to provide bank details;

530.3 another six months would be given for bank details to be provided; and

530.4 the decision was delivered in March 2021, seemingly the day it was heard, and the opportunity to claim had been live since April 2020. It was probable that creditors who had not claimed since then were unlikely to do anything now and had effectively abandoned their claim.

531 The Court consequently authorised the company to first send cheques to redress creditors who had not provided bank details, and secondly, after 6 months, if cheques remained uncashed, to

---

589 *Re Instant Cash Loans* [2021] EWHC 1164 at [13]. The orders approved by the Court involved distributing "the remaining funds to the creditors for whom it does have bank details."

590 *Re Instant Cash Loans* [2021] EWHC 1164 at [26].

distribute the remaining funds to the other creditors who had provided bank details.[591] In effect, by allowing the latter step, the Court authorised a mechanism that would close out the scheme entirely, redistributing unclaimed funds to those who had engaged with the process, despite this being outside of the contemplation of the terms of the trust.

532 Justice Green noted there was little advantage in transferring the money into court in case affected creditors might later wish to assert a proprietary claim given the remote possibility of this happening with such small sums of money,[592] and proceeded on the footing that the non-responsive creditors had effectively abandoned their claims. He observed "the practical probability is that having not done anything since April 2020, they are not going to do anything further and they have effectively abandoned their claims".[593]

533 The Court did not expressly address whether it extinguished the beneficial interests of non-claiming creditors or not. It appears to have taken the view that it did not need to do so.

534 Rather, the Court focused on the practical reality that beneficiaries had not come forward.[594] Therefore, the presence of a (legal) beneficial interest held by claimants who had not come forward was not determinative: findings of abandonment and extinguishment in fact enabled the Court to distribute otherwise than in strict accordance with the trust terms, notwithstanding that the legal interest of non-claiming beneficiaries affected by that step may have continued.

535 The Court should apply the same practical approach in respect of Cryptopia in making distribution orders in the interests of justice and finality.

---

591 *Re Instant Cash Loans* [2021] EWHC 1164 at [13].
592 *Re Instant Cash Loans* [2021] EWHC 1164 at [32].
593 *Re Instant Cash Loans* [2021] EWHC 1164 at [29].
594 *Re Instant Cash Loans* [2021] EWHC 1164 at [25]: Green J acknowledged his concern that the proposal before him "does actually overturn a beneficial entitlement", but proceeded to continue with the orders because "it seems to me that given that they have now shown that they have no intention of claiming their entitlement, they could be regarded by the court and the Company as having decided to abandon their claim."

536 In accordance with the Distribution Orders, non-claiming account holders have had ample opportunity to pursue their claims since the launch of the claims portal. Continuing to hold the trust assets for the possibility of a future claim would serve little purpose, given the chances of such a claim arising at this stage are remote.

537 The Liquidators fairly acknowledge that it is "exceedingly unlikely that the beneficial interest will ever be exhausted".[595] The liquidation will have been running for seven years as at the date of hearing, and the Liquidators have undertaken significant effort to notify account holders of the need to lodge their claims.[596] Any beneficiary claim to recover personal property held by Cryptopia on trust may therefore also be out of time in circumstances where the Hack occurred in January 2019, Liquidators were appointed in May 2019 and the claims portal has been open since the end of 2020.[597]

Distributing Trust assets to creditors

538 As above, the Court's inherent jurisdiction in *Re Benjamin*-like cases is wide in scope,[598] iterative in development, and its purpose is to enable practical difficulties to be overcome in the administration of the trust. [599]

539 As *Re Instant Cash Loans* makes clear, *Re Benjamin*-like orders are available as part of a final rather than interim distribution process. The Liquidators rely on the Distribution Orders (and the underlying jurisdiction invoked in those Orders) to support their proposal to

---

595 Liquidators' Submissions, [10.46].
596 Liquidators' Submissions, [10.45].
597 Ruscoe I, 31 July 2025, at [50]; [**201.0023**] at [**201.0038**]; Limitation Act 2010, s 31(1)(b). While beneficiaries do not have a general duty to call for a distribution, Cryptopia's accountholders did have a duty to take active steps to recover assets in circumstances where the platform ceases to operate and / or their accounts have been closed: see for example Cryptopia's terms and conditions, clause 4(c)(iii), granting account holders a 90 day window to access the platform and transfer their coins in the event their account is closed: Ruscoe I, 31 July 2025, DIR1-80; [**302.0557**] at [**302.0581**]. See also clauses 9.3(c)-(f) and 17.3 requiring account holders to take active steps regarding delisted coins and information provision respectively: Ruscoe I, 31 July 2025, DIR1-80; [**302.0557**] at [**302.0585**], [**302.0589**]. Further, the Distribution Orders require account holders to participate in the distribution process to pursue their claims. In these circumstances, any claim to require return of assets from the trustee is not open-ended. Once a beneficiary has, or ought reasonably to have, knowledge of a relevant breach, for example, the claim may become time-barred if not brought within the period prescribed by s 49(b) Limitation Act 2010; *Sain v Erceg* [2021] NZHC 761 at [62]-[64].
598 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [22].
599 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [22].

top-up each hacked trust of eligible account holders to bring the balance up to 100% of their pre-hack balance.[600]

540 The Liquidators say that because the Distribution Orders allow the Liquidators to treat non-claiming account holders as non-existent and as having abandoned their claims, and because the nature of the assets is that they are fungible and held in a common pool, the assets of those account holders may be used to meet the hacked balances.[601] The practical effect of those orders will be that the assets of non-claiming account holders will be transferred to other account holders – a step that is obviously inconsistent with the legal interest of non-claiming account holders, and in practice will completely preclude their ability to realise that beneficial interest in future.

541 GNY agrees with the Liquidators' approach on this point: treating non-claiming account holders as factually having abandoned their claims, and non-existent, means their assets can be fully and finally distributed elsewhere.

542 The only difference between the Liquidators' top-up proposal, and the use of the inherent jurisdiction to make distributions to Hack victims and creditors, is the top-up proposal will permit assets to be used to meet the entitlements of other trust beneficiaries, whereas GNY proposes that those assets should be made available to meet the liquidation claims of non-beneficiaries.

543 However, the Court's jurisdiction extends to enabling trust assets to be made available to creditors in an insolvency context such as the present.

544 Counsel for creditors in the Distribution Application referred to the case *Re Phillips* to confirm the Court's inherent jurisdiction to treat assets that were formerly part of a trust as no longer subject to that trust in some circumstances.[602]

545 In *Re Phillips*, the Court gave approval to amend the terms of a trust to allow trust assets to be removed from the trust back to the

---

600 Liquidators' Submissions, [7.57].
601 Liquidators' Submissions, [7.57].
602 Court-appointed Counsel for Creditors' Submissions dated 30 October 2023, from [4.13], citing *Re Philips New Zealand Ltd* [1997] 1 NZLR 93 (HC); [**401.0459**].

settlor company.[603] Baragwanath J considered whether this was authorised under the company's superannuation trust deed. All relevant members of the fund had consented to this amendment.

546 His Honour held that the Court "will not willingly construe a deed so as to stultify the ability of trustees, having proper consents, to amend a deed to bring it in line with changing conditions."[604] This was particularly important in the scheme of a pension trust, the terms of which should be construed to give "reasonable and practical effect to the scheme"[605] where may not have been appropriate to invoke "conventional trust principles" in light of the difficulty questions of policy and legal principle of pension trusts.[606]

547 Counsel for creditors in the Distribution Application further cited examples which confirm the Court's inherent jurisdiction to enable both trust and non-trust assets to be made available for unsecured creditor claims in the context of a liquidation.[607]

548 Contrary to the Liquidators' assertions, the fact that cases cited to support the former proposition involved Ponzi schemes with a deficient, mixed fund, where both beneficiaries and unsecured creditors had been defrauded,[608] does not make them irrelevant to the present case.

549 The Court deviated from the orthodox position in those cases as a matter of legal principle rather than fact. The difficulty and costs involved in tracing is what led the Court to conclude that pooling trust and non-trust assets was the most pragmatic approach.[609]

---

603 *Re Philips New Zealand Ltd* [1997] 1 NZLR 93.

604 *Re Philips New Zealand Ltd* [1997] 1 NZLR 93 at p 99 citing *Courage Groups Pension* 45 *Schemes* [1987] 1 All ER 528, 537.

605 *Re Philips New Zealand Ltd* [1997] 1 NZLR 93 at p 99 citing *Courage Groups Pension 45 Schemes* [1987] 1 All ER 528, 537.

606 *Re Philips New Zealand Ltd* [1997] 1 NZLR 93 at p 100 citing *Re UEB Industries Pension Plan* [1992] 1 NZLR 294.

607 Court-appointed Counsel for Creditors' Submissions dated 30 October 2023, from [4.17], citing *Graham v Arena Capital Ltd (in liq)* [2017] NZHC 973, *Re Registered Securities Ltd (in liq)* [1991] 1 NZLR 545 (CA) and *Re International Investment Unit Trust* [2005] 1 NZLR 270 (HC), where Williams J held at [49], that the question to be asked when determining possible methods of distribution is "what is the nearest approach practicable to substantial justice"; [**401.0459**].

608 Liquidators' Submissions, [10.58].

609 *Graham v Arena Capital Ltd (in liq)* [2017] NZHC 973 at [13]–[14]; *Re Registered Securities Ltd (in liq)* [1991] 1 NZLR 545 (CA) at 558; and *Re Fisk (Ross Asset Management)* [2018] NZHC 2007 at [52]–[55].

550 What underpinned this conclusion is the principle that the correct approach in equity is to select the rules which will achieve equity as between claimants depending on the context.[610]

551 In other words, the approach "that achieve[d] the least unfair result for the largest number of claimants".[611] Therefore, the departure from the orthodox position was on the premise that equity allowed for *flexibility to achieve justice* in the case at hand, as it should in the present case.

552 The principle that a trustee cannot accede or have recourse to surplus assets (raised by counsel assisting the Court) is not absolute. Maxims of equity are general principles and rules which are not required to be rigorously applied in an absolute way in all circumstances. The original purpose of equity was to modify the rigour or the common law, and rigidity in equity is not to be encouraged unless the justification for that rigidity is compelling.[612]

553 As observed by Lord Hanworth MR in *Re Wells*:[613]

> …chattels real and personal vested in a person as a trustee on private trusts which have failed are **as a general rule** held by him as trustee for the Crown as bona vacantia. The principle upon which this proposition is founded is that a trustee cannot conscientiously set up a claim to the beneficial title to the trust property as against the Crown any more than he could have set up a claim to such a title as against his cestui que trust had the trusts not failed. (emphasis added)

554 Relatedly, there is a general presumption that, where property is given to a person upon trust, the property is given to that person entirely as a trustee and not to any extent beneficially.[614] However, if the trust does not exhaust the whole beneficial interest in the property, the presumption that no beneficial interest is taken can be rebutted by an indication in the instrument of disposition that the recipient is intended to take the residue of it for his or her own benefit.[615]

---

610 *Eaton v LDC Finance Ltd (in rec)* [2012] NZHC 1105 at [59]–[61], cited in *Graham v Arena Capital Ltd (in liq)* [2017] NZHC 973 at [17] and *Priest v Ross Asset Management Ltd (in liq)* [2016] NZHC 1803, (2016) 11 NZCLC 98-046 at [106].

611 *Re Fisk* [2018] NZHC 2007 at [147].

612 *Chirnside v Fay* [2006] NZSC 68; [2007] 1 NZLR 433 at [136].

613 *Re Wells* [1933] Ch 29*, Swinburne-Hanham v Howard* [1933] Ch 29 (CA).

614 Laws of New Zealand *Trusts* at [109] and the cases cited at footnote 1.

615 Laws of New Zealand *Trusts* at [109] and the cases cited at footnote 2.

555 Those general presumptions and propositions arise in the context of an express trust created by an instrument of disposition. They are nevertheless still relevant to the present case of post-hoc, Court imposed trusts by way of the Trust Decision. As addressed elsewhere in more detail in these submissions, the Trust Decision left open a number of matters regarding the Trust terms, as those matters did not need resolution at that time.[616]

556 The exceptional circumstances of the present case, given the entirety of the context set out above, justify a departure from the general rule in *Re Wells* if required. A less rigid approach resulting in Cryptopia acceding to the surplus assets for the narrow and specific purpose of repaying outstanding creditors would be an available and principled outcome:

556.1 At a minimum there is nothing in Terms and Conditions or otherwise indicating that settlors would have been opposed to Cryptopia as trustee acceding to any surplus trust assets, for that narrow and specific purpose. That is particularly the case in the present context where the counterfactual is that the assets or their proceeds will otherwise be transferred to the Crown as bona vacantia.

556.2 As identified by counsel assisting the Court, the general rule that a trustee cannot accede to trust assets exists as a "prophylactic", to ensure that the trustee does not manipulate its management of trust assets to create a surplus of assets to which the trustee would be beneficially entitled. No such issue arises in the present case where orders that would see the trustee acceding to the surplus assets are sought only to protect creditors' interests rather than that of the trustee.

556.3 Nor does the reasoning of Lord Hanworth from *Re Wells* in respect of the general principle apply. There is no lack of conscientiousness in Cryptopia as trustee having an entitlement to surplus trust assets where such assets would be applied to meet creditor claims, where the alternative is enrichment of the Crown and substantial unpaid creditors.

---

616 See [**36**] above.

556.4 The Courts have shown a willingness to exercise a power to sanction a trustee purchasing trust property, as an exception to what had traditionally been considered the absolute nature of the rule against trustee self-dealing.[617]

557 The principle that trust assets do not form part of the estate available to meet creditor claims and the authorities cited for it (most notably *Levin v Ikiua*[618]) are of little assistance. That principle arises from different circumstances where beneficiaries with claims in the trust assets remained, unlike the present scenario (as addressed above). The essential "contest" that exists in those cases between beneficiaries and creditors does not arise in the same way in the present case.

Necessity and emergency

558 To the extent that the distribution direction amounts to an "unauthorised act" under the terms of the trust, it appears to be common ground that the Court has the inherent jurisdiction to authorise such an act in circumstances of necessity and emergency.[619]

559 This jurisdiction is engaged where the emergency may reasonably be supposed to be one not foreseen or anticipated by the author of the trust, the trustees are embarrassed by the emergency, the consent of the beneficiaries cannot be obtained to the course proposed, and the emergency must be dealt with at once.[620]

560 Curiously, the Liquidators suggest that Cryptopia's circumstances now "engages principles under the Court's inherent jurisdiction to authorise otherwise unauthorised acts of management or administration in an emergency" in order to permit a power of sale which is inconsistent with the fundamental purpose of the Trusts;[621] but at the same time, contend that no emergency arises with respect to amending the trusts to allow trust assets to be used to

---

617 Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [46-010] and [46-044]–[46-047].

618 *Levin v Ikiua* [2010] 1 NZLR 400 (HC).

619 Liquidators' Submissions, [10.70].

620 Liquidators' Submissions, at [10.70], in reliance on Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [52-001].

621 Liquidators' Submissions, [10.50].

pay creditors. The Liquidators say that "ensuring that all unsecured creditors are paid in full does not amount to an emergency", since the liquidation process itself anticipates that unsecured creditors may not be paid in full.[622]

561 Such a sanguine approach is not likely to find legitimate ways to make Hack victims whole. It is also strangely contradictory: the Liquidators cannot claim an emergency and necessity in pursuit of one result and not the other.

562 The Liquidators in fact acknowledge Cryptopia's circumstances could well be considered a case of emergency: "the Company holds assets on trust that remain unclaimed, and the beneficiaries cannot be located or identified. Something must be done with the assets so that the liquidation can be completed".[623] GNY agrees. Creditors who have gone without payment for seven years since the start of the liquidation in 2019 should receive payment.

Alpari orders

563 Notwithstanding that the Court has powers to order a final distribution without disturbing the subsisting legal interests of non-claiming beneficiaries, it also does also have a pathway to extinguishing those interests in exceptional cases. Doing so would not only permit distributions to creditors; it would also permit the certainty of finality from further claims.

564 As recognised by the Liquidators, in the *Alpari* jurisdiction the courts have made orders to the effect of terminating beneficial interests in the liquidation of corporate trustee companies.[624] For that reason, the jurisdiction has been remarked to be "entirely outwith" the *Benjamin* jurisdiction, since it alters the rights of beneficiaries.[625]

565 The *Alpari* order emerged in the United Kingdom since the enactment of the Financial Services and Markets Act 2000.[626] Such an order "contemplates a final distribution of the pooled fund

---

622 Liquidators' Submissions, [10.71].
623 Liquidators' Submissions, [10.71].
624 Liquidators' Submissions, [10.73].
625 Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [39-037].
626 Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [39-037]; *Re Alpari* EWHC (Ch) CR-2015-3442, 29 September 2016.

without regard to the date and whose claim is below a specified threshold",[627] and specifically provides that a non-responsive client or client with a minimal entitlement will cease to have an interest in the client money upon the final distribution of client money.[628] The order is enabled by way of altering the statutory trust through an executive act.[629]

566 In *Re Pritchard Stockbrokers*, the English High Court referred to the *Alpari* order.[630] The Court acknowledged a lack of prescriptive guidance in the available statutory mechanisms.[631] Accordingly, the Court assisted the joint administrators to modify client money distribution rules of the existing trust by, inter alia, introducing a bar date to claims and new rules that altered the statutory trust, such as one that "extinguished" client interests "upon the final distribution".[632]

567 While the *Alpari* jurisdiction emerges from a specific statutory context, it can and should be adopted by this Court in comparable circumstances to those addressed in the *Alpari* line of cases: distribution of significant trust assets involving a large number of non-responsive beneficiaries who have in fact abandoned their claims.

568 A significant factor which favour extinguishment is the need for finality, which applies to the present case. In *Re Pritchard*, the process of special administration had lasted more than six years. Norris J found "the need for finality is much greater than the need to preserve hitherto unpursued claims".[633] It was therefore "undoubtedly time for the book to be closed".[634] Therefore, those who received a final distribution were entitled to regard it as their

---

627 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [18].
628 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [18].
629 The Financial Conduct Authority (**FCA**) by application or consent, may direct that its rules may apply to a particular firm as required, per s 138A of the Financial Services Markets Act 2000. The FCA can accordingly alter a statutory trust by an executive act.
630 The judgment is unreported and unable to be located. The specific Order provides that a non-responsive client or a client with a minimal entitlement "shall cease to have an interest in client money within the meaning of CASS 7.17.2R(2) upon the final distribution of client money in the Client Money Trust in accordance with [the varied trust]".
631 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [12].
632 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [18].
633 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [29].
634 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [29].

own, without being exposed to a claim to follow or trace by an unresponsive client.[635]

Varying, resettling or terminating the Trusts

569 Alternatively to a distribution made without disturbing the terms of the trust, the Court may make the surplus assets available to creditors by varying the terms of the Trusts to make creditors beneficiaries of the Trusts, resettling the Trusts to achieve the same end, or terminating the Trusts entirely.[636]

Inherent jurisdiction to vary

570 The inherent jurisdiction of a Court to supervise and intervene in the administration of a trust is not affected by the TA, except to the extent the TA provides otherwise.[637] In exercising its inherent jurisdiction, a court is to have regard to the purpose and principles of the TA.[638] The relevant principles set out in the Act provide that a trust should be administered in a way that is consistent with its terms and objectives; and avoids unnecessary cost and complexity.[639]

571 The Courts have confirmed the breadth of its inherent jurisdiction to vary a trust in light of the TA. Specifically, that it may fill any "gaps" left by Parliament, as long as that is consistent with statute:[640]

> If the inherent jurisdiction takes its lead from the Court's statutory jurisdiction, it seems a more coherent approach under the 2019 Act may be to avoid strained constructions of the statutory language regarding variations to trusts and to look to the inherent jurisdiction in appropriate cases to fill any gaps left by Parliament (to the extent any such evolution of the inherent jurisdiction is consistent with the statute.

The Trusts are not "specified commercial trusts"

572 In addition to the Court's inherent jurisdiction, the TA provides a statutory mechanism for the Court to resettle, vary or terminate the trusts without the collective consent of a large class of beneficiaries.

---

635 *Re Pritchard Stockbrokers* [2019] EWHC 137 (Ch) at [29].
636 Notice of Opposition by GNY.io Limited to Originating Application for directions as to treatment of unclaimed trust assets dated 15 August 2025, at [3.18]; [**101.0016**] at [**101.0024**].
637 Trusts Act 2019, s 8(1).
638 Trusts Act 2019, s 8(2).
639 Trusts Act 2019, s 4.
640 *Re Setter* [2021] NZHC 1603 at [36(b)].

573 The Court's power to resettle, vary or terminate the Trusts arises under ss 121, 122 & 125 of the TA.

574 As a preliminary matter, GNY notes that all of these provisions apply to the Trusts. While the transitional provisions in the TA provide that ss 121 & 122 do not apply to "specified commercial trusts",[641] none of the Trusts fall within this narrow definition.

575 The "specified commercial trust" definition focusses on trusts in which the trustee and *all* the trust beneficiaries are "in trade".

576 A trust is only a "specified commercial trust" under the TA if *every* beneficiary of that trust is a beneficiary "as a result of entering into [a/the] commercial transaction that the trust is created to facilitate" per Schedule 3, cl 1. If a single person who becomes a beneficiary of a trust did not enter into a, or the, "commercial transaction" of the type that the trust was created to facilitate, the trust ceases to be a specified commercial trust.[642] A "commercial transaction" is defined to mean a transaction which *all* parties enter into "in trade". In turn, the definition of "trade" in the TA is the same as that used in the FTA, and substantively the same as the definition used in the CGA.[643]

577 It is very unlikely that *all* beneficiaries of each Trust were "in trade" when opening their Cryptopia accounts or trading on the exchange.[644]

578 Persons undertaking a transaction in their personal or private capacity - outside of their ordinary occupation or usual commercial activities - are not generally "in trade" under the FTA definition.[645]

---

641 In any event, note that ss 124 & 125 *do* apply to specified commercial trusts, and the implication is that at least the powers in s 125 are available in respect of this type of trust where a variation is sought pursuant to the Court's supervisory jurisdiction. See TA Schedule 3 cl 4(d).

642 Trusts Act 2019, Schedule 3, cl 1(2).

643 Trusts Act 2019, Schedule 3, cl 1; see FTA s 2(1) and CGA s 2(1): the CGA definition differs only in that it does not include dispositions or acquisitions of any interest in land.

644 Note that, Cryptopia's Terms and Conditions implicitly recognise this in preserving FTA and CGA liability for consumer account holders: cl 12.1(c); [**302.0577**] at [**302.0588**].

645 See discussion in Debbie Wilson "Part One: Unfair Conduct: In Trade" in *The Fair Trading Act Handbook (2018)* (LexisNexis, Wellington, 2018) at [2.70-2.85].

579 This is well-established law: the phrase "in trade" has a long history of use in New Zealand statutes. It has always been the case that whether a person is acting "in trade" is a question resolved in context, not merely by looking at the mechanics of specific transaction in question. This is why, for example, person "A" may sell a house with the intention to make a profit "in trade" if, for example, person A renovates and sells houses as a business. However, person "B" might sell the same house for profit, but may not be in trade when effecting the sale if, for example, person B lives in the house, and is selling to realise a gain on a personal asset.

580 Any Cryptopia account holders who opened their account for personal use or reasons, or to receive a gift, or to hold existing assets without trading them, or for the purposes of a hobby rather than profit (or to trade with family or friends) - or any number of other common, conceivable factual scenarios – are unlikely to have been "in trade" when they did so. Such account holders are unlikely to have entered into a commercial transaction of the kind contemplated by the TA definition of "specified commercial trusts". It also follows that it is very unlikely that any of the Trusts are "specified commercial trusts" under the TA; therefore ss 121 & 122 apply to the Trusts.

TA powers to vary, resettle or terminate

581 Sections 121 and 122 of the TA codify the common law rule in *Saunders v Vautier* permitting termination and (final) distribution of a trust if all legally capable adult beneficiaries call for its termination:[646]

581.1 section 121 requires a trustee to terminate the trust and distribute the trust property on being required to do so by all beneficiaries who hold beneficial trust property; and

581.2 section 122 allows a trustee to vary the terms of the trust or consent to the resettlement of the trust upon unanimous consent of beneficiaries.

---

646 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [10.2.2]; *Saunders v Vautier* (1841) Cr & Ph 240, 49 ER 282.

582 The same conditions apply for both sections: every beneficiary must consent, the trustee must receive a request from or on behalf of each beneficiary, and, if there are beneficiaries who are not competent to consent, do not yet exist, or will acquire a beneficial interest in the future,[647] the Court must make an under granting approval on behalf of those beneficiaries. This is done under s 124.

583 Section 125 is a new power that did not exist in the Trustee Act 1956. It enables the Court to "waive the requirement that a beneficiary consent to the termination of a trust under section 121 or the variation or resettlement of a trust under section 122".[648]

584 The effect of s 125 is to widen the scope of the exception to the pre-existing requirement that all beneficiaries who together hold all of the beneficial interest in the trust property must consent to any termination, variation or resettlement of a trust. Where a Court orders a waiver of consent of some or all beneficiaries, the trustees can proceed with varying the trust using the power conferred on them by s 122, and to terminate the trust under s 121.

585 While s 124 specifically addresses beneficiaries who are not competent to consent, do not yet exist, or will acquire a beneficial interest in the future, s 125 does not specify the type of beneficiary. Instead, commentators observe the power is intended to address circumstances where there are adult beneficiaries with full capacity who are difficult to locate, are part of a disparate group, simply fail to response, or refuse to consent to what is proposed, i.e. "elusive, un-cooperative or dissenting beneficiaries".[649]

586 Section 125 empowers the Court to waive consent requirements for the variation, resettlement or termination of the Trusts.

---

647 Trusts Act 2019, s 124 together with s 122(2)(c).
648 Trusts Act 2019, s 125(a). Under s 125(2), an application for an order for the waiver may be made by the trustees or any person with a beneficial in the interest in trust property.
649 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [10.10].

587 The present situation fits within the situations contemplated by the Law Commission in recommending empowering the Court in accordance with s 125, namely, to prevent:[650]

> … desirable variations being thwarted in situations where *one or more ascertainable beneficiaries cannot be traced or contacted despite reasonable efforts*, or to deal with situations where there are *numerous beneficiaries with a remote or negligible interest in a trust*. In such situations it is impractical and costly to require the personal consent of each of them. We consider that it is unreasonable to allow people with interests of a *remote or negligible nature* to have the *power of veto over variations that are desired by beneficiaries with far more significant interests*.
>
> (emphasis added)

588 In present circumstances, it is impracticable for all beneficiaries to consent to the termination, variation, and resettlement of the trusts, especially given that non-claiming account holders have not engaged in the distribution process.

589 The Liquidators' suggestion that s 125 may only be invoked in narrow circumstances is not persuasive.[651] The Liquidators fairly acknowledge "there is no dispute the consent of beneficiaries cannot be obtained".[652] The beneficiaries of the unclaimed holdings are ineligible account holders who have failed to register in or complete the claims portal, despite several attempts by the Liquidators to contact over the course of seven years.[653]

590 This situation is therefore precisely what the Law Commission contemplated when envisaging ascertainable beneficiaries who cannot be contacted despite reasonable efforts, or numerous beneficiaries with a remote or negligible interest. It would simply be impractical and costly to require each of their personal consent.[654]

591 Section 125 allows the court to waive the requirement that "a beneficiary", in other words, *any beneficiary*, consent to the termination, variation or resettlement of a trust. Furthermore, the

---

650 Law Commission *Review of the Law of Trusts: A Trusts Act for New Zealand* (NZLC R130, 2013) at [10.14].
651 Liquidators' Submissions, [10.65(c)]–[10.68].
652 Liquidators' Submissions, [10.65].
653 Liquidators' Submissions, [10.65].
654 Law Commission *Review of the Law of Trusts: A Trusts Act for New Zealand* (NZLC R130, 2013) at [10.14].

Law Commission envisaged waiving the requirement of consent "of any other person".[655]

592 There is nothing in the wording of s 125 to suggest the section may only be only invoked in the narrow circumstances where the proposed amendment has been put to all account holders and agreed to by one class of beneficiaries. The section is meant to adequately cater for a "range of situations" where the consent of beneficiaries cannot be reasonably obtained, a lacuna left unaddressed in s 64A of the Trustee Act 1956.[656] The Law Commission acknowledged the concern that this approach would allow far-reaching revisions of trusts, but still considered it preferable to leave it to the court to determine whether it should in all the circumstances approve an arrangement that extends beyond or differs from what the settlor may have wished.[657] The Court is given a wide latitude under this section.

No impact on vested interests in trust property (variation)

593 Section 125(4) provides that the Court must not make an order of waiver of consent to a variation, resettlement or termination of a trust if its effect would be to reduce or remove any vested interest in the trust property.

594 An order varying the Trust terms to add additional discretionary beneficiaries to the Trusts under s 122 will not offend s 125(4). Adding an additional beneficiary with no fixed interest in trust assets does not, per se, displace the interests of current beneficiaries. The beneficiaries' interest can be expressed as residual, and would not, therefore, displace any vested or unvested interest in trust property.

595 Adding creditors including Hack victims as beneficiaries would, however, position the trustee to directly invoke the principles in *Re Benjamin*, and *In Re Instant Cash Loans*, and relied on in the Distribution Orders, to enable final distributions of trust assets. This

---

655 Law Commission *Review of the Law of Trusts: A Trusts Act for New Zealand* (NZLC R130, 2013) at [10.14].
656 Law Commission *Review of the Law of Trusts: A Trusts Act for New Zealand* (NZLC R130, 2013) at [10.09].
657 Law Commission *Review of the Law of Trusts: A Trusts Act for New Zealand* (NZLC R130, 2013) at [10.12].

will be possible, because the company creditors will all be trust beneficiaries.

596 Specifically, pursuant to orders akin to those made in the Distribution Judgment, the trustee could proceed to make final distributions on the basis that:

596.1 non-eligible account holders have "abandoned" their claims in fact; and

596.2 such claims are not, in fact, "in existence".

597 Unclaimed trust assets would, in that scenario, be available to meet the claims of creditors by way of trust distribution, consistently with well-established trust law. Eligible account holders will have had their claims satisfied from the trust assets, and creditor beneficiaries will be able to receive distributions from surplus assets, as the trustee is entitled to proceed on the basis that no other claims are in existence. In this respect, varying the Trusts to make all creditors a beneficiary of the Trusts will not offend s 125(4), and will ultimately facilitate an outcome akin to that sought by the Liquidators in their "top up" proposal for solvent trusts.

No vested interests in trust property

598 In any event, resettling (or varying) the Trusts with the effect of making creditors including Hack victims beneficiaries of the Trusts would not have the effect of removing or reducing - or even diluting - the non-claiming account holders' interests in the Trusts.

599 This is because it is doubtful whether those who are required by Court order to be treated as factually non-existent and to have abandoned their claims in trust property have a vested interest in any trust assets.

600 A vested interest is an interest which is not subject to any condition precedent.[658] A beneficiary may have a vested interest in trust assets even though he or she is not entitled to immediate enjoyment of those assets under the terms of the trust. A vested interest may be vested in interest or in possession: the

[658] Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [1-048].

latter confers an immediate right to present enjoyment of the property while the former confers a present right to future enjoyment. By contrast, a contingent interest is one which will not vest unless and until some requirement other than the determination of a prior interest, is satisfied. This includes attainment of some specified age, or survival to a particular time, or the occurrence of some external event,[659] such as attaining rights upon vesting day.[660]

601 It is an important feature that the nature of the non-claiming account holders' current interests has now been subjected to an order from the court under its inherent jurisdiction and / or s 136 of the TA to be treated as "not in existence".

602 Counsel are not aware of any case law which directly addresses the issue of whether an order confirming factual abandonment of claims and factual non-existence of interests would still constitute a vested interest in trust property. However, non-claiming account holders cannot be said to have a vested interest in the trust assets as a result of these orders. Now that the Final Cut-off Date has passed, a non-claiming account holder who now wishes to establish their interest in the trust assets does not have a present right to future enjoyment of the assets as of right, let alone an immediate right to present enjoyment of the property. Their interest is contingent on a further process of the court.

603 In connection with this issue, it is notable that the present situation does not fit the policy rationale for s 125(4). The Law Commission envisaged s 125(4) to be for the protection of the "recalcitrant adult beneficiary" with a "fixed or indefeasible interest" where he or she refuses to consent to a variation.[661] The present situation is clearly not that of a recalcitrant adult beneficiary, rather, after ample opportunity provided to complete the claims process, have been explicitly ordered by Palmer J to be treated as having their claims abandoned and not in existence.

---

659 Lynton Tucker, Nicholas Le Poidevin and James Brightwell *Lewin on Trusts* (20th ed, Thomson Reuters, London, 2019) at [1-048].

660 *Ma v Guo Liang Maand Lk Trustees (No 91) Ltd (as trustees of Good Hope Trust)* [2016] NZHC 1426 at [20].

661 Law Commission *Review of the Law of Trusts: A Trusts Act for New Zealand* (NZLC R130, 2013) at [10.15].

Factors in s 125(3)

604 In assessing whether an order under s 125 is appropriate to facilitate a variation or resettlement of the Trusts to broaden the scope of beneficiaries, the Court is required to take into account the following factors:

604.1 the nature of any person's interest in the trust property and the effect of the proposed order on that interest;

604.2 the benefit or detriment that may result to any person with an interest in the trust property if the court makes or refuses to make the proposed order; and

604.3 the intentions of the settlor of the trust in settling the trust, if it is practicable to ascertain those intentions.

605 None of these factors are determinative. Rather they are matters that should be considered in the exercise of the Court's discretion. The first two factors are of relevance here.

606 As noted earlier, the third factor is not a feature of the known context of the Trusts, nor a feature of the reasoning in the Trust Decision's findings on the intention to establish a trust per cryptocurrency as opposed to, for example, per account, or for all accounts on the exchange: the difference in scope being the number of other beneficiaries in each trust.

607 The purpose of the first factor is to consider the interests of all the ascertained and unascertained beneficiaries who have or may acquire an interest in the trust property and assess the effect that granting or refusing the waiver would have on any of those interests.[662]

608 When considering these two factors, the more remote the interest is of the beneficiaries on whose behalf the waiver is sought, the more likely the court may be to grant the waiver. For example, in *Talijancich v Talijancich*,[663] the Court granted the waiver of consent for the contingent discretionary beneficiaries of the trust. The Court

---

662 Nicola Peart (ed) *Family Law: Family Property* (online ed, Thomson Reuters) at [TRU.125.05].

663 *Talijancich v Talijancich* [2021] NZHC 753.

considered those beneficiaries were extremely unlikely ever to benefit from the trust, because the class of primary discretionary beneficiaries was large and the contingent beneficiaries would benefit only if there were no surviving primary beneficiaries.

609 Similarly, the non-claiming account holders in the present case are also unlikely to benefit from the respective Trusts.

610 The Liquidators acknowledge that in all likelihood, few account holders will reach out to prove their entitlement to the trust property given that the liquidation has been running for seven years, the Liquidators have undertaken significant effort to notify account holders of the need to lodge their claims, and it becomes more difficult for account holders to prove ownership of their account as time goes on.[664] Varying the Trusts would therefore have little to no practical effect on any person's interests in trust assets, whether that be a benefit or detriment, given nature of the non-claiming account holders' interests as factually non-existent, and the practical reality of the abandoned claims.

Expiry and vesting in Cryptopia

611 In the alternative to terminating, resettling or varying the Trusts, the Court could declare that the Trusts have expired.

612 As noted earlier, the Trust Decision left open a number of matters regarding the Trust terms, as those matters did not need resolution. One of those matters was the duration of the Trust. The TA specifies that the maximum duration of a Trust is 125 years.[665] However, the "terms of a trust may specify or *imply* a shorter duration".[666] As is clear from the s 16(3) of the TA, the implied end date of a trust can be either a date, or a mechanism or means for determining a date. The terms of a Trust can, of course, specify or imply an expiry date notwithstanding that beneficiary interests exist: if the Trust expires, the trustee must distribute the assets in accordance with the terms of the Trust.

---

664 Liquidators' Submissions, [10.45].
665 Trusts Act 2019, s 16(1).
666 Trusts Act 2019, s 16(2).

613 On this topic, the Terms and Conditions imply that the settlors did not intend for the Trusts to continue operating indefinitely in circumstances where the exchange platform is defunct. In particular, under Cryptopia's terms and conditions:

613.1 clause 1B allowed the account holder to "buy, sell and exchange supported Coins through the Platform" and to "store supported Coins in our hosted Wallets."[667]

613.2 under clauses 4.3(a)(vii) and 4.4(a)(viii), users contemplated the company closing or suspending accounts where it was no longer able to "reasonably provide the Account or any Services as a result of any resource constraint, technical failures or other difficulties in providing the Platform";[668] and

613.3 under clause 4.4(c)(iii), after the closure of any account, users were given 90 days to access the platform to transfer coins or redeem fiat pegged tokens. All access to the platform was lost after that period.[669]

614 The effect of Cryptopia's insolvency, the Trust Decision, and subsequent the Distribution Orders, have somewhat modified the specifics of these contractual expectations, but the orders sought to date are not inconsistent with them. Rather, the process of proscribing a Final Cut-off Date for claims is consistent with the expectation in the Terms & Conditions that account holders would have a fixed period to claim tokens in the event that the exchange ceases to operate. At that point:

614.1 the functional purpose of the trust ceases;

614.2 the accounts - from which Cryptopia's trustee obligations to beneficiaries are derived - are closed;

614.3 the beneficiaries have had a fixed period of time to realise their beneficial interests; and

---

667 Ruscoe I, 31 July 2025, DIR1-80, Terms and Conditions, clause 1B; [**302.0577**].
668 Ruscoe I, 31 July 2025, DIR1-82, Terms and Conditions, clauses 4.3(a)(vii) and 4.4(a)(viii); [**302.0577**] at [**302.0579**].
669 Ruscoe I, 31 July 2025, DIR1-84, Terms and conditions, clause 4.4(c)(iii); [**302.0577**] at [**302.0581**].

614.4 the Trustee may deny those beneficiaries access to the platform – and their tokens – in perpetuity.

615 The inference is that:

615.1 the Trusts expire; and

615.2 the residual (and final) beneficiary (following the period afforded to account holders to realise their assets) is Cryptopia.

616 This does not, of course, amount to Cryptopia acceding to Trust assets *as trustee*. Rather, its status as residual beneficiary arises by implication from the terms of the Trust itself.

617 Finally, termination of the Trusts under s 121 or the Courts' inherent jurisdiction may lead to the same outcome of the surplus assets vesting in Cryptopia. Section 121 does not stipulate that the trust property must be distributed directly to the beneficiaries, so beneficiaries can still direct how the trustees might distribute the trust after termination, including to a new trust,[670] or to Cryptopia. Of course, it is not practicable to seek the consent of all account holders.[671]

618 The Court is empowered to waive the requirement for beneficiary consent under s 125.

Transferring surplus assets to the Crown

619 Against the options outlined above, the Liquidators propose that the Court confers a power of sale on the trustee to facilitate recourse to s 149.

Section 149 is discretionary & undesirable

620 While the Courts have previously found that a transfer to the Crown may be appropriate in scenarios where beneficiaries do not engage

---

670 Andrew Butler (ed) *Equity and Trusts in New Zealand* (3rd ed, Thomson Reuters, Wellington, 2025) at [10.2].

671 See above discussion at [**590**].

with trustees,[672] s 149 does not impose any requirement on a trustee to transfer undistributed trust property to the Crown.

621 Transfer of undistributed trust property to meet unpaid creditor claims is preferable to transfer to the Crown. As the English High Court determined in *Re Instant Cash Loans*,[673] transferring the unclaimed funds under this power was "clearly a last resort if nothing else was possible" and that "it is, according to the authorities, to be discouraged".[674]

622 The English High Court considered there was little advantage in paying the money into court in case the affected beneficiaries might wish later to assert a proprietary claim, given they were unwilling to engage with the process by providing bank details or cashing a cheque, their entitlements were for a small amount of money, and it would be completely disproportionate for a claim to be asserted at that stage.[675]

623 The process of transferring assets to the Crown in this case similarly ought to be viewed as a last resort.

624 This is the ordinary approach of the New Zealand courts. For example, the Courts have rejected transferring residual trust property under s 149 of the TA where evidence had been provided that settlors did not intend for trust assets to be distributed to the Crown, notwithstanding that a trust beneficiary refused to engage with the trustee over an extended period, and notwithstanding that something needed to be done with trust assets.[676]

---

672 See, for example, *Public Trust v Gargan* [2013] NZHC 1058, where the beneficiaries could be found, but refused to accept payment. The Court directed for surplus funds to be transferred to Public Trust under s 77 of the Trustee Act 1956 (predecessor of s 149).

673 In the context of determining whether to make alternative directions to pay the surplus of the unclaimed funds to the Court under s 63 of the Trustee Act 1925 (UK). Section 63(1) provides: trustee, or the majority of trustees, having in their hands or under their control money or securities belonging to a trust, may pay the same into court.

674 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [23].

675 *Re Instant Cash Loans* [2021] EWHC 1164 (Ch) at [32].

676 In *Re Holland* [2023] NZHC 464, one of the two residuary beneficiaries of the estates had been located but refused to respond to multiple enquiries over an extended period of years (from 2009 to 2022). A trustee provided an affidavit testifying that he strongly believed the settlors would not have wanted a half share of their estates to go to the Crown, and would instead have wanted it to go to the other residual beneficiary. Based on this evidence, Jagose J, who had originally contemplated a transfer to the Crown under s 149, instead made an order under s 136 authorising the trustee to distribute the estates as if that beneficiary did not

625 As noted earlier, there is limited available evidence of settlor intention. However, if anything, the fact that Cryptopia's Terms and Conditions clearly provided for account holders to lose access to their coins and the platform if they did not retrieve those coins when the platform ceased to operate[677] suggests that transfer to the Crown was not contemplated.

626 A useful analogy is found in the Companies Act. Section 316 of the Companies Act allows liquidators to transfer "unclaimed assets of a company standing to the credit of a liquidator" after completion of the liquidation to be paid to Public Trust, who then pays the balance to the Liquidation Surplus Account after 12 months after deducting any required to meet claims.[678] Although this section concerns company rather than trust assets, the cases which deal with this section shows courts are hesitant to deprive creditors and "waste" unclaimed assets by transfer to the Liquidation Surplus Account.

627 In *Waller v Kiwi International Airlines*,[679] the Court approved a transfer to the Liquidation Surplus Account on the basis that there were a large group of creditors with claims greater than the comparatively small surplus, and unresolved practical difficulties facing distribution. As a result, it was debatable whether there would be any funds available for creditors at all after a distribution process. The consequence of this would "treat all unsecured creditors equally: with an equal sharing of misfortune".[680]

628 In contrast, in *Tasman Pacific Airlines v New Zealand Airline Pilots' Association*,[681] the Court rejected the liquidator's application to transfer unclaimed assets to the Liquidation Surplus Account. In

---

exist. In *Fowler v Hizo* [2024] NZHC 3881, the Court granted an order under s 136 to distribute a 1/4 share of a deceased's estate belong to a missing beneficiary to be divided and added proportionally to other beneficiaries. In this case, counsel argued that a clause in the will specifically providing that a failed share was to be divided and added to the other shares in the same portion was evidence that the settlor did not intend for the share to be transferred to the Crown as non-distributable property under s 149.

677 Ruscoe I, 31 July 2025, DIR1-82, terms and conditions, clauses 4.3(vii) and 4.4(viii); [**302.0577**] at [**302.0580**].

678 Companies Act 1993, s 316. Money held in the Liquidation Surplus Account may be vested in accordance with the Trusts Act 2019, paid to anyone entitled to payment or distribution, or paid to meet the claims of creditors or legal costs.

679 *Waller & Anor as Liquidators of Kiwi International Airlines Ltd (In Liquidation)* HC Auckland CIV 2005-404-7051, 26 July 2006.

680 At [29].

681 *Tasman Pacific Airlines of NZ Ltd (in liq) v New Zealand Airline Pilots' Association* HC Auckland CIV-2009-404-90, 27 July 2009.

that case, there was a "not insignificant amount" of $150,000 that could be available for creditors. The Judge noted that under s 253 of the Companies Act, the liquidators had a principal duty to realise and distribute the net assets to the creditors in a reasonable and efficient manner. The Court rejected the liquidator's argument that it would be uneconomic to distribute small amounts of sums. Instead, the Court considered that was to be balanced by the consideration that such a distribution was "the only way that the larger creditors can get what is rightfully theirs … Better that some money is wasted so some collect, rather than it all be 'wasted'… by being paid into the [Liquidation Surplus Account]".[682]

629 Therefore, unlike in *Waller* where a small surplus meant all unsecured creditors would share equal misfortune, in *Tasman Pacific Airlines*, granting the orders would result in misfortune which would be unfairly extended to all as "some unsecured creditors who would otherwise receive payments will miss out because of the futility of distributing to others".[683]

630 The Court did not look favourably at the prospect of the only beneficiary being "the liquidation account, that offers nothing to any creditor"[684] and found it unreasonable and inefficient to give the liquidation surplus account a "boon" while depriving some creditors of significant payments to which they are entitled.[685] The liquidator's application was dismissed. Instead, the Court allowed the liquidators to pay surplus funds to the liquidation surplus account only after all unsecured creditors had been given a reasonable opportunity to accept their payments.[686]

631 Those cases are consistent with a general reluctance to transfer unclaimed assets to the Crown when there are available, and credible alternatives.

682 At [19].
683 At [18].
684 At [18].
685 At [20].
686 At [21].

Power of sale

Section 149 is unavailable on its face

632 In any event, s 149 is not available. Subsection (1) permits a trustee who is administering trust property that the trustee is not able to distribute in accordance with the terms of the trust to transfer that trust property to the Crown, but only "if the trust property consists of money or of financial products that can legally be transferred to the Crown."[687]

633 GNY agrees with the Liquidators that property may only be transferred to the Crown under s 149 if it consists of money or other financial product that can be legally transferred.[688] Coins held on the Cryptopia platform do not constitute money or a financial product.[689] Thus, the assets may only be transferred to the Crown if converted to fiat currency, an act which is procedurally unclear.

634 GNY also agrees that the same difficulty is encountered with the Unclaimed Money Act 1971, which only applies to money, which cryptocurrency is not.[690] Thus, the same procedural challenge of transfer arises.

Power of sale unavailable or inappropriate

635 This unavailability of s 149 compels the Liquidators propose that the Court confers a power of sale on the trustee. This is the key context in which the Liquidators seek a power of sale.

636 As the Liquidators acknowledge, the Terms and Conditions do not provide any express power to Cryptopia to sell the cryptocurrencies held on trust.[691] This is unsurprising, as the primary purpose of the Trusts is to hold cryptocurrency and deal with it as directed by beneficiaries. The authors of *Lewin on Trusts* opine that "[t]he court has… no inherent jurisdiction to permit the sale of trust property contrary to the terms of the trust, even though it would be for the benefit of all persons interested".[692]

---

687 Trusts Act 2019, s 149(1).
688 Liquidators' Submissions, [10.7].
689 Liquidators' Submissions, [10.8].
690 Liquidators' Submissions, [10.15].
691 Liquidators' Submissions, [10.20].
692 Liquidators' Submissions, [10.20].

637 The Liquidators therefore seek:

637.1 a direction from the Court confirming such a power of sale exists under s 56 of the TA, which grants trustees "all powers necessary to manage the trust property" and "all the powers necessary to carry out the trust". In seeking that, the Liquidators acknowledge the power to sell trust property may be inconsistent with Cryptopia's role as a bare trustee for which its primary obligations are to hold the trust property and deal with it by account holders;[693] or

637.2 if the Court does not find Cryptopia has a power of sale, that the Court in its discretion may extend the Trustees' powers to allow for a power of sale under s 130 of the TA or the Court's inherent jurisdiction.

638 Section 130 allows the Court to vary or extend a trustee's powers if the Court considers the variation or extension is necessary or desirable for the property management and administration of the trust property, the variation or extension does not alter a beneficiary's interest under the trust; and the variation or extension does not involve a power to distribute trust property to a beneficiary.[694]

639 GNY raises four points in response.

640 First, the flexibility, creativity and initiative displayed by this submission would be better employed in support of distributing surplus assets to render Hack victims whole.

641 Second, there is no basis to invoke s 56. It has never been "necessary" that the trustee of the Trusts hold a power of sale in order to "manage" Trusts property nor to "carry out the trust". A power of sale is the inconsistent with the central purpose of the Trusts, and Cryptopia's primary obligation to hold cryptocurrency for account holders. In this respect, GNY agrees with the Liquidators' responsibly acknowledged reservation as to whether it could credibly be said that s 56 has impliedly conferred a power of sale on the

693 Liquidators' Submissions, [10.25].
694 Trusts Act 2019, s 130.

trustee with respect to Trusts established for the express purpose of holding cryptocurrency assets;

642 Third, a court should not lightly exercise its discretion to confer a power of sale on a bare trustee under s 130 or under any inherent or other jurisdiction.

643 There is case law under the comparable section of s 130 TA, s 64 Trustee Act 1956,[695] which supports the view that where the identity or type of trust asset is important to the trust settled by the settlor or to a beneficiary a Court will not lightly order a sale.[696]

644 In this case, it is not appropriate for the proper management and administration of the Trusts to make an order of this kind in the all the circumstances. "Necessity" is a high bar, and needs to be considered in light of other, viable alternatives for dealing with the unclaimed trust assets, which there are here – including the powers of distribution, variation, resettlement, termination or expiry identified above. Desirability is also not met in all the circumstances, including the long-standing judicial reluctance to transfer assets to the Crown other than by way of last resort, and the low likelihood that assets transferred in this manner will ultimately be distributed to account holders who have not engaged with the claims process over several years to date.

645 Finally, the Liquidators' necessity submission (that the sale power should be permitted under s 130 out of necessity for the administration of the trust property)[697] conflicts with the Liquidators' contrary position on necessity in other respects. The true position is

---

695 Trustee Act 1956, s 64: "subject to any contrary expressed in the instrument (if any) creating the trust, where in the opinion of the court any sale…. is expedient in the management or administration of any property vested in a trustee, or would be in the best interests of the persons beneficially interested under the trust, but it is inexpedient or difficult or impracticable to effect the same without the assistance of the court, or the same cannot be effected by reason of the absence of any power for that purpose vested in the trustee by the trust instrument (if any) or by law, the court may by order confer upon the trustee, either generally or in any particular instance, the necessary power for the purpose, on such terms, and subject to such provisions and conditions (if any) as the court may think fit, and may direct in what manner any money authorised to be expended, and the costs of any transaction, are to be paid or borne, and as to the incidence thereof between capital and income…"

696 In *Re Smith* [1975] 1 NZLR 495 (HC),the Court declined to approval the sale of a farm property pay beneficiaries under a will, as the testator clearly intended for the farms to be settled. In *Re Nichols (dec'd)* HC Dunedin M104/96, 18 March 1999, the Court declined to approve a sale of property to improve income, as it was clear the settlor intended that the trustee maintain the assets during the trust period.

697 Liquidators' Submissions, [10.41].

that there is an emergency of a sufficient kind to permit the Court to stand back and appropriately exercise its inherent jurisdiction in the interest of justice.[698]

Liquidators' arguments support GNY's position

646 Finally, some of the Liquidators' reasons as to why conferring a power of sale and ordering a transfer pursuant to s 149 is preferred are equally applicable to GNY's proposal that the surplus assets may be made available to Hack victims and creditors. Conversely, the Liquidators' reasons as to why making the assets available to creditors is *not* an appropriate course of action may also apply to their suggested transfer to the Crown.

Pragmatism

647 First, the Liquidators cite pragmatism as a reason for why the sale of cryptocurrencies is necessary and / or desirable.[699] Yet the interests of pragmatism also support making unclaimed assets available for creditors.

648 For example, the Liquidators appear most concerned with protecting account holders' beneficial interests and their right to receive a distribution; they suggest it is appropriate to transfer the property to the Crown and invoke the Court's jurisdiction under s 130 to extend the trustee's powers to allow for a power of sale.[700]

649 However, at the same time, the Liquidators acknowledge that it is "exceedingly unlikely that the beneficial interests will ever be exhausted".[701] There may therefore be little practical utility in transferring the assets to the Crown (and that position is particularly stark given the very real possibility that Hack victims and creditors would then be left with their claims unresolved, despite the surplus).

---

698 In the Distribution Judgment, Palmer J permitted the sale of cryptocurrency to fiat currency on the basis of necessity in order to transfer such currency to restricted jurisdictions where transfer of cryptocurrency would constitute a criminal offence (*Ruscoe v Houchens* [2024] NZHC 419 at [24]); [**401.0503**] at [**401.0513**]. The necessity for the power of sale in that situation is distinct to the present situation, as the sale was necessary for the liquidators to fulfil their obligations to distribute trust property.

699 Liquidators' Submissions, [10.44].

700 Liquidators' Submissions, [10.40].

701 Liquidators' Submissions, [10.45]–[10.46].

Substratum

650 Despite acknowledging the substratum concept may not be useful as it is possible that this law will no longer be followed in New Zealand,[702] the Liquidators suggest that granting a power of sale would not invalidate the substratum of the Trusts.[703] At the same time, they imply that amending the terms of a trust to allow trust assets to be used to pay creditors would constitute an amendment to the substratum of the Trusts.[704]

651 Since the substratum equates to "the trust's underlying purposes, objects and substance",[705] it is not clear how converting the subject matter of the Trust and removing the trustee-beneficiary relationship entirely by transfer to the Crown would not disturb the Trusts' underlying purposes, objects and substance.[706] Leaving aside the issue of whether changing the subject matter of the Trusts disturbs the substratum, the submission does not address the result of the sale, which is to transfer the property to the Crown so that Cryptopia is discharged from further responsibility with regard to the trust property.[707]

Emergency

652 As above, an emergency arises with respect to Cryptopia's circumstances in their entirety. The Liquidators say there is an emergency because "the Company holds assets on trust that remain unclaimed, and the beneficiaries cannot be located or identified. Something must be done with the assets so that Cryptopia's liquidation can be completed".[708] This factor applies in equal measure to making the assets available for creditors.

Procedural and doctrinal difficulty

653 Enabling a power of sale in this instance is procedurally difficult for the reasons identified above, including by the Liquidators.[709] In

---

702 Liquidators' Submissions, [10.37]–[10.38].
703 Liquidators' Submissions, [10.49].
704 Liquidators' Submissions, [10.69].
705 *Holland v Jonkers* [2021] NZHC 3469 at [166].
706 Which, as a bare trust, entails holding property on trust for the absolute benefit and at the absolute disposal of other persons, see *Halsbury's Laws of England* (4th ed, 2001) at [650].
707 Trusts Act 2019, s 149(5).
708 Liquidators' Submissions, [10.71].
709 Liquidators' Submissions, [10.25] and [10.39]. The Liquidators acknowledge the power to sell trust property may be inconsistent with Cryptopia's role as a bare trustee and have not identified any cases where a power of sale has been granted without beneficiaries consenting or being represented at the hearing.

seeking orders granting a power of sale, the Liquidators acknowledge the novelty of no trust deed proscribing the powers and duties on Cryptopia as a trust,[710] and having to resort to the court's inherent jurisdiction as a basis for recognising the power.[711]

654 Such an approach is in sharp contrast with the Liquidators' opposition to any departure from orthodoxy which would make trust assets available to resolve Hack victim and creditor claims.

Orders under s 151(2)(a)

655 Finally, GNY notes that in the event that the Court is minded to confer a power of sale to transfer assets to the Crown under s 149, this can be achieved in a pragmatic manner, consistent with the statute, that makes assets available to Cryptopia's creditors. Specifically, s 151 enables a wide statutory discretion as to the terms on which a transfer of trust assets could occur.

656 Where a transfer to the Crown occurs, the trust assets remain trust property. However, the Crown is "not subject to the duties or liabilities of a trustee in respect of any transferred property".[712] The Crown is *in loco* trustee in respect of such trust property, not an actual trustee: the TA confirms that the Crown receives and is required to maintain the trust assets subject to statutory duties (i.e. s 151(2)), not trustee duties.

657 Under s 151(2)(a), the Secretary to the Treasury is required to deal with the transferred property in accordance with any court order made by the court in relation to the transferred property.

658 S 149 TA provides a pragmatic mechanism for trustees who are unable to distribute trust property, and to discharge that trustee from further liability.[713] It follows that the s 151(2) discretion can be exercised pragmatically to meet the justice of the situation at hand. That can be a wide-ranging discretion given the Crown does not become a trustee of the relevant trust assets. Court orders can

---

710 Liquidators' Submissions, [10.39(c)].
711 Liquidators' Submissions, [10.34].
712 Trusts Act 2019, s 151(6).
713 Trusts Act 2019, s 149(5).

be made under s 151(2)(a) which reflect the pragmatic context in which the statutory power arises.

659 If the Court decides to transfer the surplus assets to the Crown under s 149, GNY therefore seeks that the Court make a further order under s 151(2)(a) requiring the Crown to make immediate payment of assets to Cryptopia. A payment of this kind would be available to meet creditor claims against the company. Such orders are appropriate:

659.1 in the context set out in these submissions, where non-claiming account holders have abandoned the benefit of each trust and Hack victims and creditors do not otherwise stand to recover their losses; and

659.2 as against the Crown, which has indicated to the Liquidator that it is content not to be heard on the terms of the orders sought, and which has no actual interest in the assets in question. The order proposed under s 151(2)(a) would have no impact on the Crown, other than imposing a discrete obligation to make a specific, identified payment.

SECTION 11: ADDITIONAL MATTERS

660 The Liquidators raise various additional matters in this proceeding. To the extent those matters are not addressed in GNY's notice of opposition and these submissions, they do not relate to or concern GNY's claim against Cryptopia.

661 GNY in any event wishes to comment briefly on the following points.

Assignment of account holder claims

662 The Liquidators consider that Cryptopia's terms and conditions prevent any assignment of account holders' claims.[714] And the Liquidators point to concerns they have regarding verification of account holders' identify and compliance matters, as a practical reason why, in their view, assignments of claims should not be permitted.

663 GNY considers Cryptopia's terms and conditions do not prohibit the assignment of a creditor claim in Cryptopia's liquidation.

664 Regardless of whether this is the case, Cryptopia's terms and conditions clearly do not prohibit the assignment of *proceeds* of any claim against Cryptopia. That is a separate issue to the assignment of "rights or obligations" under the terms and conditions.[715] And, in GNY's submission, assignment of the proceeds of a claim does not trigger any of the practical concerns regarding claimant identification which the Liquidators rely on to oppose assignment of claims more generally.

Trusts with surpluses

665 GNY agrees with the Liquidators that the surplus holdings in trusts in which actual cryptocurrency holdings exceed the amounts recorded in Cryptopia's internal database should not be distributed to eligible account holders.

666 This is because account holders should receive distributions calculated on the basis of their admitted claim, not windfall distribution of surplus trust assets:

---

714 Liquidators' Submissions, [7.32].

715 Ruscoe I, 31 July 2025, DIR1-93, terms and conditions, updated 7 August 2018, clause 18.2(b); [**302.0577**] at [**302.0590**].

666.1 to which they have no beneficial entitlement; and which

666.2 are in excess of their admitted claim.

667 GNY agrees with the Liquidators that these surplus holdings should be treated as company property. Those company funds could then be made available for other account holders and/or Hack victims to satisfy their claims and beneficial entitlements.

668 Another option would be for the Trusts with those surplus holdings to be resettled and / or varied, in order to make the funds available for other creditors and / or Hack victims (in the same manner in which GNY suggests in section 10 above).

669 GNY also agrees with the Liquidators that a pragmatic approach is warranted in this instance. Moreover, if a pragmatic approach is taken in this instance regarding the surplus holdings, there appears to be no reason why a pragmatic approach should not also be adopted with regards to the unclaimed assets from non-claiming account holders. Both approaches have the effect of treating assets that were formerly part of a trust as no longer subject to the trust.

Dated: 11 May 2026

D Kalderimis KC / L L Fraser / J Marcetic / L C Bercovitch
Counsel for GNY

SCHEDULE 1: TABLE OF PLEADINGS AND SUBMISSIONS

GNY's position	GNY's position	Liquidators' position
GNY as an account holder		
The two accounts GNY operated and traded were GNY accounts, not personal accounts of its directors and founders.	GNY's subs, section 4 NOO: 3.14, 3.15	Liqs' subs, [8.25] – [8.43]
Cryptopia's liability for Hack losses		
Cryptopia is in breach of its fiduciary, statutory, contractual and tortious duties to GNY and other Hack victims.	GNY's subs, section 5 and section 6 NOO: 3.1 – 3.9	Liqs' subs, [8.68] – [8.232], [9.1] –[9.27] Application: 2.3, 2.10
Effect of Cryptopia's exclusion clauses		
The exclusion clauses are irrelevant to several of GNY's claims by virtue of the source of Cryptopia's obligation, which cannot be contracted out of; they are irrelevant to the balance of GNY's claims because they are ineffective when tested against the law concerning onerous exclusion clauses.	GNY's subs, section 7 NOO: 3.10 – 3.13	Liqs' subs, [8.44] – [8.67] Application: 1.1 -1.3
Valuing GNY's claims in BTC		
It is legally appropriate to measure and pay GNY's claim in BTC, not NZD.	GNY's subs, section 8 NOO, schedule: item 2.2	Liqs' subs, [8.276] – [8.291] Application: 2.2
The value of GNY's claim		
The value of GNY's claim, as assessed by its expert evidence is 337.92 BTC for the stolen LML tokens claim and 1,421.44 BTC for the lost market capitalisation claim.	GNY's subs, section 9 NOO, schedule: item 2.10(f)	Liquidators' submissions, [8.292] – [8.341] Application: 2.10(f)

Distribution of surplus trust assets		
Unclaimed trust assets should be made available to Cryptopia's creditors, including Hack victims, rather than transferred to the New Zealand Crown.	GNY's subs, section 10 NOO, 3.17 – 3.24	Liqs' subs, section 10 Application: 8.1 – 8.6
Assignment of account holder claims		
GNY has not purported to assign its account holder claim. However, GNY considers Cryptopia's terms and conditions do not prohibit the assignment of the proceeds of any creditor claim in Cryptopia's liquidation.	GNY's subs, section 11 NOO, schedule: item 4	Liqs' subs, [7.32] – [7.42] Application: 4.1
Trust with surplus amounts		
GNY agrees with the Liquidators that surplus holdings in trusts should be treated as company property, instead of being distributed to eligible account holders. Alternatively, trusts with surplus holdings may be resettled / varied in order to make the funds available to creditors and / or Hack victims	GNY's subs, section 11 NOO, schedule: item 7.1	Liqs' subs, [7.23] – [7.48] Application: 7.1

SCHEDULE 2: CHRONOLOGY

Red highlighting = events relating to GNY

Date	Event	Reference
29 July 2014	Cryptopia incorporated.	[redacted] 18. [302.0904]
2016	[redacted] a company which used machine learning models to help accurately predict customers' actions.	[redacted] at [6]. [201.0001] at [201.0002]
2017	[redacted] created an account with Cryptopia [redacted]	[redacted]-077 [302.0959] at [302.0967]
Nov 2017	Cryptopia initially engaged Pulse Security to diagnose existing vulnerabilities in its cybersecurity posture.	Ruscoe 2, DIR2-65 [301.0130]
14 Nov 2017	Pulse report raised serious concerns about the inadequacy of Cryptopia's cybersecurity arrangements and identified numerous material weaknesses in Cryptopia's basic security settings.	Ruscoe I, DIR1-111 – 119 [301.0137]
29 Nov 2017	Pulse report described penetration test: it was able to penetrate and enter Crptopia's wallet without detection.	Ruscoe I, DIR1-120 [301.0147]
20 Dec 2017	Pulse report: "Web Application Penetration Testing and Source Code Review", identifying one high severity and 16 medium vulnerabilities.	Ruscoe I, DIR1-142 [301.0173]
2018	[redacted].	[redacted], at [7]. [201.0001] at [201.0003]
24 Feb 2018	Cryptopia's Operations Manager warned its senior managers and directors that they should not be	Ruscoe II, DIR2-296-298 [301.0276]

Date	Event	Reference
	able to sleep at night because of the critically vulnerable state of the platform's security.	
26 Feb 2018	FMA email to Cryptopia addressing concerns about Cryptopia, expecting Cryptopia to develop *"a full suite of disclosures to accurately and fairly describe the services provided and in particular the risks involved"*.	Ruscoe II, DIR2-342 [**301.0279**]
28 Feb 2018	Pulse report described a further penetration test, whereby it, again, penetrated and entered Cryptopia's wallet without detection.	Ruscoe I, DIR1-182 [**301.0282**]
~ March 2018	New Zealand government advised Cryptopia it was an identified cyberattack target, and at imminent risk of an attack occurring. GSCB also met with Cryptopia's directors to explain the imminent threat.	Ruscoe I, at [73]–[74] [**201.0023**] at [**201.0043**] DIR2-200-201 [**301.0072**]
1 March 2018	Pulse report: "Lancaster Firewall Incident Forensic Review", in response to a potential security breach in the firewall.	Ruscoe I, DIR1-214 [**301.0314**]
9 March 2018	Pulse report: review on publicly available information about Cryptopia staff online.	Ruscoe I, DIR1-222 [**301.0325**]
16 March 2018	Pulse report: "Password Cracking Engagement Results". Pulse was able to crack passwords belonging to Cryptopia users.	Ruscoe I, DIR1-253 [**301.0363**]
21 March 2018	The FMA engaged with Cryptopia regarding *"concerns we've previously raised"*. The FMA requested that Cryptopia directors provide an 'attestation' in relation to Cryptopia's systems against malicious online attacks, including that it had never been successfully hacked.	Ruscoe II, DIR2-345 [**301.0367**]

Date	Event	Reference
26 March 2018	Pulse report: "Wallet Segregation Testing". Pulse simulated a compromised wallet being deployed by Cryptopia and raised concern that *"an attacker exploiting the issues identified would likely to be able to access the [Remote Procedure Call] services belonging to other cryptocurrency wallets, and thereby transfer funds out of these wallets".*	Ruscoe I, DIR1-255 [**301.0367**]
17 April 2018	Cryptopia executed a proposal from Technical Security Services to perform a security review.	Ruscoe II, DIR2-262 [**301.0397**]
20 April 2018	Risk Statement published on Cryptopia's website (29 April 2018 is the earliest date this is able to be found on Cryptopia's archived website).	Ruscoe I, at [34], DIR1-104 [**201.0023**] at [**201.0034**] and [**301.0413**]
26 April 2018	Cryptopia's directors declined to provide the requested attestation to the FMA and instead agreed to provide a letter *"setting out the views of management and its Board regarding the adequacy of its current security processes".*	Ruscoe II, DIR2-350 [**301.0443**] at [**301.0445**]
29 April 2018	Pulse report: "VPN Segregation Testing" noting there was *"insufficient network segregation between users of the VPN and the Cryptopia environment".*	Ruscoe I, DIR1-265 [**301.0428**]
30 April 2018	Pulse report: "April 2018 Phishing Forensic Review" in response to two phishing emails sent to an employee.	Ruscoe I, DIR1-280 [**301.0452**]
30 April 2018	Cryptopia letter to the FMA: *"As far as we are aware Cryptopia has never been successfully hacked from a malicious external party".*	Ruscoe II, at DIR2-357 [**301.0001**]
12 May 2018	Pulse report: "SQL Monitor Web Application Penetration Testing", whereby Pulse identifies a	Ruscoe I, DIR1-288 [**301.0465**]

Date	Event	Reference
	number of serious vulnerabilities in the SQL Monitor web application.	
17 May 2018	Cryptopia prepared "Infrastructure Plan" which contained recommendations relevant to enhancement of security, but the author of the document did not clearly consider the failed Pulse penetration tests.	Ruscoe I, DIR1-351 [**301.0490**]
By June 2018	Cryptopia's directors and senior managers had excluded Cryptopia's most senior technical staff from its senior leadership team.	Ruscoe I, DIR1-357 [**301.0490**]
10 July 2018	Pulse report: "10th July Security Incident CISO Report".	Ruscoe I, DIR1-307 [**301.0116**]
7 Aug 2018	Pulse report: "Service Now Web Application Penetration Test".	Ruscoe I, DIR1-315 [**302.0593**]
7 & 8 Aug 2018	Cryptopia introduced revised terms and conditions. An email to account holders explaining those new terms said: "*We take your security and personal information very seriously and these revised Terms and Conditions more clearly outline our policies and obligations to you.*"	Ruscoe I, DIR1-80, DIR1-99-100 [**302.0577**] [**302.0606**]
8 Aug 2018	Mr Nicholson email to Cryptopia director, Peter Dawson, warned of some of the concerning consequences of Cryptopia's decision to remove technically expert staff from senior leadership discussions.	Ruscoe II, at DIR2-329 [**302.0608**]
10 Aug 2018	Pulse report: "Intermediate Wallet Solution Testing". Pulse raised concerns that sensitive information could be available to unauthenticated users.	Ruscoe I, DIR1-324 [**302.0610**]

Date	Event	Reference
5 Oct 2018	Pulse emailed Cryptopia about vulnerability of the wallet environment for coin delisting, being *"not fit for purpose from a security perspective"*.	Ruscoe II, DIR2-174 [**302.0683**]
15 Oct 2018	[redacted] approached Cryptopia on behalf of GNY about listing LML on the platform.	Sibenik I, PJS1-15. [**302.0718**]
18 Oct 2018	GNY submitted its listing application for the LML token.[716]	Sibenik I, PJS1-8. [**302.0719**]
24 Oct 2018	Pulse report: review of the Virtual Chief Information Security Officer role and state of information security within Cryptopia, advising *"Cryptopia is far from the level of security maturity required for a cryptocurrency exchange"*, and *"further work is required before confidence another similar attack [simulation] could be prevented"*.	Ruscoe I, DIR1-345 [**302.0729**]
5 Nov 2018	Cryptopia advised [redacted] that GNY's proposal had *"passed our project review and is ready to progress"*. Cryptopia provided the Listing Quote for the LML project, setting out the terms and pricing options for the listing.	Sibenik I, [redacted]-20 Listing Quote: [redacted]-1 [**302.0732**]
	GNY accepted the Listing Quote.	Sibenik I, [redacted]-28 [**302.0745**] at [**302.0748**]

[716] The Liquidators suggest [redacted] was incorrect to say in his evidence that the LML tokens were not part of GNY's Initial Coin Offering: Liquidators' Submissions, [8.19]-[8.21]. [redacted] explains that GNY's ICO was for the sale of GNY tokens, which are ERC20 tokens on the Ethereum Network. At the time GNY submitted its listing request in 2018, its ICO of the GNY token was underway to get the GNY business off the ground; the LML token was to be created the following month, on 14 November 2018: Sibenik I, 1 August 2025, [redacted]-8; [**302.0719**] at [**302.0722**]. The listing form was clear on its face. Like the GNY token, LML was also an ERC20 token on the Ethereum Network: [redacted] 30 March 2025, [10]; [**201.0012**] at [**201.0014**]. [redacted] evidence also explains that the GNY and LML tokens are linked: [redacted], 30 March 2025, [8], [**201.0001**] at [**201.0003**].

Date	Event	Reference
	Cryptopia confirmed that [redacted] had already completed level 2 KYC verification in 2017.	Sibenik I, PJS1-28 [**302.0745**] at [**302.0748**]
16 Nov 2018	GNY paid the listing fee of 3.3m DOT.	Sibenik I, PJS1-26 [**302.0745**] at [**302.0746**]
19 Nov 2018	Cryptopia confirmed that *"LML has made it through our Code Review process".*	Sibenik I, PJS1-25. [**302.0745**]
21 Nov 2018	Cryptopia confirmed the LML wallet built had been successful and was ready to be listed on Cryptopia.	Sibenik I, PJS1-50 [**302.0770**]
Late Nov 2018	[redacted] created an account with Cryptopia [redacted]	[redacted] at [9] [**201.0001**] at [**201.0003**]
26 Nov 2018	GNY listed its LML tokens on Cryptopia.	Sibenik I, PJS1-50. [**302.0770**]
14 Jan 2019	Hack of Cryptopia. All of GNY's LML tokens on Cryptopia were stolen.	[redacted] at [14-15] [**201.0001**] at [**201.0004**]
7 March 2019 to 20 March 2019	GNY corresponded with Cryptopia about the stolen LML tokens that had made their way onto the Bitbay exchange, and which Bitbay had temporarily frozen. Bitbay could not permanently block the trading in those tokens without Cryptopia's assistance. Cryptopia did not assist Bitbay as it was asked to.	[redacted] at [16-17], [redacted] at 29-50 [**201.0001**] at [**201.0004**] and [**302.0865**].

Date	Event	Reference
18 March 2019	[redacted] wrote to Cryptopia outlining the severe challenges GNY was facing as a result of the Hack.	[redacted] at [20] [**201.0141**] at [**201.0145**] [redacted] at CW1-46. [**302.0887**]
11 April 2019	GNY issued proceedings against Cryptopia in the Christchurch High Court.	[redacted], at [26]; [redacted] at 9. [**201.0001**] at [**201.0006**] and [**302.0912**]
14 May 2019	Cryptopia placed into liquidation.	Ruscoe I at [7]. [**201.0023**] at [**201.0035**]
10 July 2019	GNY submitted its creditor claim form to the creditors.	[redacted] at [28], [redacted]-1 at 51-66 [**201.0001**] at [**201.0006**] and [**302.0949**]
8 April 2020	*Ruscoe v Cryptopia* [2020] NZHC 728 released.	Prior Casebook [**401.0365**]
21 July 2020	GNY issued a notice of failure to comply under the Companies Act.	[redacted]1 at 93. [**303.1023**]
31 July 2020	Liquidators confirmed their "*preliminary assessment is that [GNY] is a creditor of Cryptopia in relation to account holder losses and*	[redacted]- 1 104 [**303.1034**]

Date	Event	Reference
	it is working through issues associated with the quantum of the claim to be admitted".	
Dec 2020	Liquidators' claims portal opened for account holders.	Ruscoe, 31 July 2023 at [50] Prior Casebook [**401.0648**]
18 Dec 2020	Chapman Tripp letter to Buddle Findlay advising GNY does not consider it necessary to register on the claims portal and requesting confirmation of that point.	[**401.0589**] at [**401.0613**]
10 Feb 2021	Buddle Findlay email to Chapman Tripp: *"The liquidators have confirmed to us that they require your client to register on the claims portal in the same way as all other account holders".*	[**401.0589**] at [**401.0615**]
24 Feb 2021	Chapman Tripp letter to Buddle Findlay confirming GNY would register on the claims portal as the Liquidators had informed was required, and that correspondence between Chapman Tripp and Buddle Findlay about GNY's claim should take precedence over any information provided through the claims portal.	[**401.0589**] at [**401.0618**]
3 March 2021	Buddle Findlay letter to Chapman Tripp advising, in respect of the claims portal, *"your client will need to go through this process for both of the accounts that it had".*	[**401.0589**] at [**401.0620**]
29 May 2023	GNY initiated a token swap, to swap all outstanding LML tokens into the GNY tokens.	[redacted] at [24] [**201.0001**] at [**201.0005**]
1 March 2024	*Ruscoe v Houchens (Distribution)* [2024] NZHC 419 released.	Prior Casebook [**401.0503**]
31 March 2025	Soft Cut-Off Date for the Liquidators' distributions process.	Ruscoe I at [18].

Date	Event	Reference
		[**201.0023**] at [**201.0028**]
31 March 2025	GNY filed an application for orders requiring confirmation of its claim under the Companies Act.	Prior Casebook [**401.0540**]
30 Sept 2025	Final Cut-Off Date for the Liquidators' distributions process.	Ruscoe I at [17]. [**201.0023**] at [**201.0028**]