Electronically issued / Délivré par voie électronique : 30-Oct-2026
Superior Court of Justice - Toronto - Civil / Cour supérieure de justice

Court File No./N° du dossier du greffe: CV-26-00021630-00CP

Court File No

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N :

MARCOS ROBERTO BENEDETT

Plaintiff

- and -

COINKITE INC., RODOLFO NOVAK, and PETER D. GRAY

Defendants

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

TO THE DEFENDANTS:

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiffs. The Claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a Statement of Defence in Form 18A prescribed by the Rules of Civil Procedure, serve it on the Plaintiff's lawyer or, where the Plaintiff does not have a lawyer, serve it on the Plaintiff, and file it, with proof of service, in this Court office, WITHIN TWENTY DAYS after this Statement of Claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your Statement of Defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a Statement of Defence, you may serve and file a Notice of Intent to Defend in Form 18B prescribed by the Rules of Civil Procedure. This will entitle you to ten more days within which to serve and file your Statement of Defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT WILL BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

TAKE NOTICE: THIS ACTION WILL AUTOMATICALLY BE DISMISSED if it has not been set down for trial or terminated by any means within five years after the action was commenced unless otherwise ordered by the court.

Date: October 30, 2026

Issued by: _____

Courthouse:
330 University Avenue
Toronto, Ontario M5G 1R7

TO: Coinkite Inc.
3219 Yonge Street, Unit 376
Toronto, Ontario M4N 3S1

AND TO: [redacted]

AND TO:

CLAIM

1. The Plaintiff, Marcos Roberto Benedett, claims on his own behalf and on behalf of the Class (as defined below) against the Defendants:

    a. an order certifying this action as a class proceeding, and appointing Marcos Roberto Benedett as the representative plaintiff for the Class and Diamond & Diamond Lawyers LLP as Class Counsel;

    b. as against the Defendant Coinkite Inc.:

        i. a declaration that Coinkite:

            1. engaged in unfair practices contrary to section 17(1) of the *Consumer Protection Act, 2002* (***"CPA"***);

            2. owed the Plaintiff and the Class a duty of care in the design, manufacture, and supply of its COLDCARD Wallets (defined below) and associated software and firmware, and to warn them of defects affecting their security, and breached those duties of care; and

            3. breached the express and implied warranties and conditions governing the sale of COLDCARD Wallets and associated software and firmware, contrary to sections 14 and 15 of the *Sale of Goods Act*, R.S.O. 1990, c. S.1 (***"SGA"***);

        ii. aggregate damages in the amount of $300,000,000 for:

            1. negligence;

            2. negligent misrepresentation;

            3. breach of contract;

4. breach of s. 17(1) of the *CPA* in accordance with s. 18 and/or rescission under s. 18; and
5. breach of warranty in accordance with s. 51 of the *SGA*;

iii. aggravated and punitive damages in the amount of $100,000,000;

c. as against the Defendants Rodolfo Novak and Peter D. Gray:

i. a declaration that Novak and Gray are personally liable to the Plaintiff and the Class for the matters pleaded and damages sought in this Claim;

ii. further or in the alternative, a declaration that the corporate veil of Coinkite ought to be pierced so that Novak and Gray are jointly and severally liable for Coinkite's liabilities to the Plaintiff and the Class;

d. a reference or such other directions as may be necessary to determine issues not determined at the trial of the common issues;

e. an order waiving any notice requirements pursuant to s. 18(15) of the *CPA*;

f. pre-judgment and post-judgment interest pursuant to the *Courts of Justice Act*, R.S.O. 1990, c. C.43;

g. costs of notice and administering the plan for distributing recovery in this action, pursuant to ss. 22 and 26 of the *Class Proceedings Act,* 1992, S.O. 1992, c. 6;

h. costs of this action on a full indemnity basis, inclusive of all disbursements and HST; and

i. such further and other relief as counsel may advise and this Court may permit and deem just and appropriate in the circumstances.

OVERVIEW

2. Beginning on July 30, 2026, unknown attackers stole approximately 1,800 Bitcoin, worth more than US$110 million at the time, from wallets secured by Coinkite's COLDCARD hardware devices, including those of the Plaintiff and other Class Members. Coinkite marketed COLDCARD wallets as providing exceptional and superior security against Bitcoin theft.
3. The thefts were made possible by a basic, preventable defect in the devices' firmware, which generated predictable recovery seeds (explained below), and therefore reproducible private cryptographic keys, that attackers could reconstruct and exploit without access to the devices (the *"***Defect***"*).
4. The COLDCARD wallet's sole purpose was to keep the private keys (as explained below) to access the owner's Bitcoin secure. The Defect defeated the one function the device existed to serve. The thefts were the very losses the Defendants promised to prevent, and the owners bought the wallets to prevent them.
5. The Defect arose and persisted because the Defendants failed to design, test and maintain the COLDCARD wallets properly and adequately, and then failed to repair the Defect or warn their customers even after becoming aware of it in May 2025.
6. By early August 2026, investigators had traced the theft of the Bitcoin across thousands of Bitcoin addresses, making it one of the largest reported hardware-wallet compromises of 2026.
7. The breach was exacerbated by the fact that the Defendants: (i) knew, or ought to have known, of the Defect more than a year before the breach, yet failed to correct it; (ii) failed to take adequate steps to notify or warn affected users once the breach was discovered; (iii) marketed and sold the COLDCARD based on safety and security features it did not, in fact, have; and (iv) held Coinkite out as a leader in Bitcoin security and hardware.

8. The Plaintiff brings this action on his own behalf and on behalf of the proposed class of COLDCARD purchasers defined below for the relief set out in paragraph 1 above.

THE PARTIES

The Proposed Representative Plaintiff

9. Marcos Roberto Benedett is a 41-year-old resident of Brazil.

10. In November 2021, Marcos purchased a COLDCARD wallet from Coinkite. Marcos generated the Seed Phrase securing his Bitcoin on that device. On August 2, 2026, the Bitcoin secured by that Seed Phrase was transferred without his authorization or consent, in a single mass-sweep transaction that also drained 795 other addresses, and has not been recovered to date.

The Class

8. The proposed Class (collectively the *"***Class Members***"*) is defined as follows:

> All persons, other than Excluded Persons, who owned Bitcoin that was at any time secured by a recovery seed generated on a COLDCARD hardware wallet running any of the following firmware versions, and whose Bitcoin was transferred without their authorization on or after July 30, 2026:
>
> (a) for COLDCARD Mk2 and Mk3 devices, firmware versions 4.0.0 through 4.1.9, inclusive;
>
> (b) for COLDCARD Mk4 and Mk5 devices, standard firmware versions preceding 5.6.0 or Edge firmware versions preceding 6.6.0X; and
>
> (c) for COLDCARD Q devices, standard firmware versions preceding 1.5.0Q or Edge firmware versions preceding 6.6.0QX (*"***Affected Devices***"*).
>
> *"*Excluded Persons*"* means the Defendants, their respective employees, Coinkite's officers, directors, and any entity in which a Defendant holds a controlling interest.

The Defendants

9. Coinkite is an Ontario corporation with its head office in Toronto. Coinkite designs, manufactures, markets, sells and supplies Bitcoin hardware and security devices to consumers in Canada and around the world, including the COLDCARD. Coinkite describes itself on its website as a *"leader in Bitcoin security and hardware."*

10. The Defendant, Rodolfo Novak, resides in Toronto and is the co-founder, director, and the Chief Executive Officer of Coinkite. He is well-known in cryptocurrency circles — and is referred to in this pleading — as NVK.

11. At all material times, NVK was the Chief Executive Officer of Coinkite and exercised management, direction and control over its operations, including the development, marketing and sale of COLDCARD products. NVK also personally made public representations concerning the security and reliability of COLDCARD, including through his personal social media accounts.

12. The Defendant, Peter D. Gray, also resides in Toronto and is the co-founder and Chief Technology Officer of Coinkite. He plays an essential role in managing and directing Coinkite.

13. Gray personally authored and controlled the firmware code that gave rise to the Defect. In or around May 2025, an independent developer reported the flaw in COLDCARD's Seed Phrase generation to Gray. Despite this warning, Gray failed to take reasonable steps to investigate or correct the Defect, or to warn users of the risk.

FACTS

Crypto-Assets, Bitcoin, Blockchain and Digital Wallets

14. There are four technological terms that are most material to this class proceeding: crypto-assets; Bitcoin; blockchain; and digital wallets.

15. **Crypto-assets** exist only in digital form. They use cryptography to secure transactions and are recorded on a blockchain maintained by a peer-to-peer network of computers. The main type of crypto-asset is cryptocurrency, such as Bitcoin and Ether.

16. **Bitcoin** is the first and best-known cryptocurrency. It came into existence in 2008. Bitcoin is a

digital crypto-asset not issued by any government, bank, or central organization. It operates under the open-source protocol of the decentralized, peer-to-peer Bitcoin network, which maintains a public ledger online of confirmed Bitcoin transactions known as the "blockchain."

17. A **blockchain** is a shared, online public record of transactions. Computers in the network (i) verify each transaction, (ii) group transactions into time-stamped blocks, and (iii) link each block to the one before it, forming a chain. Because many computers keep copies of the record, it is very difficult to alter. Once a transaction is recorded on the blockchain, it generally cannot be changed or reversed.

18. Despite the name, a **digital wallet** does not hold crypto-assets. A wallet holds the digital keys that control the asset, but the assets themselves are recorded on the blockchain. There are two kinds of digital keys, public and private. For each digital wallet, a specific public and private key are created and are mathematically tied together:

    a. a **public key**, similar to an email address, is used to create addresses for receiving crypto assets, and those addresses are visible and identify wallets on the blockchain;

    b. a **private key**, similar to a password, is secret and is stored in a wallet and used to authorize transfers of the associated crypto assets. A private key authorizes transfers of crypto assets. Whoever holds the private key controls the assets. Only the person with the secret private key associated with the assets can access and move them. This is explained further below.

19. There are two kinds of wallet, hot and cold:

    a. **hot wallets** are connected to the internet, such as wallets managed by a trading platform (e.g., Coinbase);

    b. **cold wallets** keep private keys offline, usually on a dedicated physical device.

20. COLDCARD is a cold wallet.

COLDCARD and Seed Phrases

21. The COLDCARD generates a confidential recovery phrase (the *"***Seed Phrase***"*), from which the COLDCARD derives the user's secret private keys. As noted, each private key has a corresponding public key, from which one can generate Bitcoin addresses.

22. Bitcoin addresses and their balances are publicly visible on the Bitcoin blockchain. The public-private key relationship works in one direction: a person can derive a public key from its private key, but cannot realistically reconstruct the private key from the public key.

23. A user will disclose their (public) Bitcoin address to receive Bitcoin without compromising the private key needed to spend it.

24. Importantly, the Bitcoin network accepts any transaction authorized with the correct private key. It does not verify the identity or require the consent of the owner.

25. Anyone who reproduces a user's Seed Phrase can therefore derive the user's private keys, identify the associated Bitcoin holdings, and thereby transfer them without the owner's consent.

26. The security of those holdings depends on randomness, i.e., the Seed Phrase being generated unpredictably, so that no one else can reproduce it: an attacker who can reproduce the Seed Phrase can derive the identical private keys and authorize transactions without ever possessing the wallet.

The COLDCARD's Purpose: To Prevent Theft

27. The COLDCARD's purpose is to keep the Seed Phrase, and therefore the private key derived from it, secret and secure.

28. There are three essential components to COLDCARD's security promise: randomness of the

Seed Phrases it generates, disconnection from the internet, and complete secrecy. Accordingly, the COLDCARD is purportedly designed to:

a. generate a truly random Seed Phrase, from which the user's private keys, public keys, and Bitcoin addresses are all derived;

b. hold the resulting private key beyond the reach of the internet, by being a *"cold"* wallet; and

c. ensure Seed Phrase secrecy, to ensure that a user's Bitcoin can be moved only by someone in possession and control of the device itself.

29. Users purchased, and reasonably expected, the COLDCARD to place their Bitcoin beyond the reach of cyberattacks and theft.

30. The Defendants market and represent the COLDCARD as a personal hardware wallet that secures its users' Seed Phrase and the private keys derived from it through a random process that no one else can reproduce, so that only a person in possession of the device can access and transfer the Bitcoin it protects.

31. But, from March 2021, as it became publicly known in July 2026, COLDCARD failed to do the very thing it was created to do. Firmware issued by Coinkite caused affected devices to generate Seed Phrases that were not truly random and were, in effect, predictable. This was the Defect.

32. The Defect allowed third parties to reproduce users' Seed Phrases, derive their private keys, and transfer the users' Bitcoin without authorization, defeating the primary protection the device existed to provide.

Origin of the Defect

33. The Defect originated in a software integration error introduced in the COLDCARD in

March 2021, when Coinkite migrated the COLDCARD to new software.

34. The error affected seed generation on the Mk2 and Mk3 COLDCARD models running firmware versions 4.0.1 through 4.1.9. Seeds generated on the later Mk4, Mk5, and Q models before corrected firmware was integrated were also affected.

35. The Defect lay in the software build-and-link process. Instead of building the Seed Phrase drawn from the COLDCARD's dedicated hardware random number generator, as the COLDCARD wallet was originally designed, the seed generation routine was erroneously linked to a general purpose, non-cryptographic software pseudorandom number generator: MicroPython's *"*Yasmarang*"* generator.

The Defect's Consequences

36. As a result of the Defect, the Seed Phrases the COLDCARD produced were significantly more predictable and less random than represented, and could be reproduced by attackers without accessing the devices.

37. The vulnerability did not weaken the cryptography itself. The private keys remained of ordinary cryptographic size, but the *"*entropy*"*, or measure of randomness, of the Seed Phrase generation process was drastically reduced.

38. As a result, the *"*search space*"* — the number of possible Seed Phrases — an attacker had to test shrank from the intended 128 bits to what Coinkite estimates is as little as about 40 bits for the Mk2 and Mk3, and about 72 bits for the Mk4, Mk5 and Q. Each lost bit halves the number of possible Seed Phrases.

39. A reduced search space is increasingly vulnerable to a determined attacker.

40. Modern computing power can search a 40-bit space through systematic trial and error (a *"*brute-force attack*"*). At a rate of one billion guesses per second, searching every possibility

would take about 18 minutes for a 40-bit space, compared with about 150,000 years for a 72-bit space.

41. But 72 bits is Coinkite's own estimate, and the actual search space may be far smaller where an attacker can narrow down when and how a device generated its Seed Phrase. Even at 72 bits, the search space is about 72 quadrillion times smaller than the 128-bit search space the COLDCARD devices were promoted and represented to provide.

The Defect Did Not Appear Suddenly

42. The Defect remained in the COLDCARD's seed generation software for more than five years, from the March 2021 migration until Coinkite released corrected firmware in late July 2026, as the thefts were underway.

43. Any device that generated a seed during that period would produce a compromised Seed Phrase. Once generated, such a Seed Phrase remained vulnerable even if the device was later updated, because a firmware update cannot add randomness to a private key that already exists.

44. Since at least May 2025, the Defendants were aware of the Defect.

45. The Defendants took no steps to investigate or correct the Defect, to warn users, or to correct their representations, and continued to market and sell the COLDCARD as *"ultra-secure"*.

How the Attackers Engineered the Thefts

46. The unknown attackers exploited the defective seed-generation process without ever directly accessing victims' hardware wallets.

47. The attackers proceeded, in substance, in four steps:

    a. **Reproducing vulnerable Seed Phrases**. Working offline, the attackers reproduced the defective Seed Phrase generation process and likely generated all possible Seed

Phrases.

b. **Deriving keys and addresses**. For each candidate Seed Phrase, they derived the corresponding private keys and Bitcoin addresses using standard, publicly known methods.

c. **Identifying funded addresses**. They compared the derived addresses against the public blockchain to identify addresses holding Bitcoin.

d. **Transferring the Bitcoin**. After reconstructing the private keys, they used them to authorize transactions that transferred the Bitcoin to addresses they controlled.

48. The resulting transactions were cryptographically valid, because the attackers held the private keys needed to produce valid signatures. The Bitcoin network would not and could not distinguish their transactions from those authorized by the rightful owners.

49. The attackers therefore needed nothing from the owners or their devices. They did not need the owners to disclose their Seed Phrases; they did not need to access the owners' computers or connect to their COLDCARDs; and they did not need the owners to approve any transaction.

50. The crucial failure — the Defect — had already occurred when the COLDCARD generated a Seed Phrase that was insufficiently unpredictable.

51. To date, the stolen funds have not been recovered.

Disclosure of the Hack and Coinkite's Acknowledgments and Repair

52. Following the breach and the Bitcoin thefts, Coinkite posted an acknowledgment on the COLDCARD GitHub repository — COLDCARD's publicly accessible online software code collection — stating that *"versions from 2021 to July 2026 had a bug which produced poor entropy"*.

53. On July 30, 2026, while the thefts were still underway, Coinkite publicly disclosed in a security advisory on its website that a firmware bug had caused weakened seed generation, which attackers exploited to steal funds.

54. In a technical backgrounder published the same day, Coinkite further acknowledged that *"a complex and subtle series of bugs prevented the hardware [Random Number Generator] from contributing randomness in certain versions of the firmware"*.

55. After disclosing the Defect on July 30, 2026, Coinkite began emailing customers the next day, in batches, and only to addresses it could reach through its store and newsletter systems.

56. Owners whose addresses were not in those systems, including some who purchased through resellers, received no direct warning from Coinkite. Even owners whose addresses Coinkite held may not have received or acted on the emails in time. Addresses dating back years may have been outdated, and messages may have been filtered as spam.

57. An unexpected email urging owners to move their Bitcoin also resembled a common phishing scam. Coinkite itself had to confirm publicly that the emails were legitimate. Owners who did not receive the warnings, or reasonably distrusted them, could therefore have remained unaware of the danger until their Bitcoin was stolen.

58. By August 1, 2026, an estimated 1,367 BTC had already been stolen, while Coinkite's notification efforts were underway.

59. Coinkite also initially advised owners that its newer models were unaffected, an assessment it subsequently reversed.

60. On or around July 30–31, 2026, Coinkite released updated firmware for the Affected Devices.

61. As noted, the firmware update did not repair a Seed Phrase that had already been generated using affected firmware. Such a Seed Phrase remained vulnerable, and the owner's Bitcoin

remained at risk until the owner generated a new Seed Phrase on a secure device and transferred the Bitcoin to addresses derived from the new Seed Phrase.

The Defendants' Pre-Existing Knowledge of the Defect

62. The Defendants knew, or ought to have known, of the Defect well before the breach.

63. In a panel transcript that Coinkite published in its newsletter on January 20, 2023, NVK acknowledged that a bad device or software *"could create bad entropy ... either by bug or by a malicious intent."* Later, in the same discussion, NVKwarned that *"if you have a low entropy Bitcoin key, someone will take those funds from you"*.

64. In the same discussion, NVK represented that Coinkite guarded against this risk because Coinkite *"mix[es] the entropy of different chips manufacturers"* so that those manufacturers would all have had to conspire together to compromise it, and *"on top of that, they would have to cheat our openly verifiable source code."*

65. The Defendants therefore knew, no later than January 20, 2023, two years after the Defect was introduced into COLDCARD, that weak entropy was a known failure mode that could expose users' funds to theft, and represented that the COLDCARD protected against it. Yet they failed to detect and prevent the Defect.

66. In or around May 2025, an independent Bitcoin developer, James O'Beirne, audited the COLDCARD's firmware and warned Gray of the flaw in its seed generation.

67. According to Mr. O'Beirne, Gray *"shrugged off"* his report.

CAUSES OF ACTION

Breach of the Consumer Protection Act, 2002, S.O. 2002, c. 30

68. The Defendants engaged in unfair practices in breach of s. 17(1) of the *CPA* by making false, misleading and deceptive representations as defined in s. 14.

69. The Plaintiff and Class Members were *"consumer[s]"* and the Defendants were *"suppliers"* within the meaning of s. 1 of the *CPA*.

70. The Plaintiff's and Class Members' purchase of the COLDCARD from the Defendants were *"consumer transactions"* and *"consumer agreements"* within the meaning of s. 1.

71. The Defendants engaged in the unfair practices under the *CPA* between October 2021 and July 2026**,** through marketing and publications on Coinkite's website, and on platforms including X and GitHub in April to July 2026.

72. The Defendants represented that COLDCARD had performance characteristics, benefits, and qualities that it did not have, and that it met a standard of quality that it did not meet.

73. Specifically, the Defendants represented that COLDCARD generated each user's Seed Phrase using high-quality, device-generated randomness, so that the Seed Phrase was unique and could not be reproduced by anyone else.

74. That representation was false since, because of the Defect, COLDCARD was generating predictable Seed Phrases, enabling attackers to reconstruct those phrases and steal users' Bitcoin.

75. The full particulars of the representations the Defendants made that constitute unfair practices are known to the Defendants and were widespread. They include, non-exhaustively:

    a. **On the Coinkite website and COLDCARD product pages:**

        i. *"COLDCARD is the world's most trusted and secure Bitcoin signing device a.k.a Bitcoin hardware wallets"* (April 2022- July 2026), and *"Coldcard is the world's most trusted and secure Bitcoin hardware wallet"* (November 2021-April 2022);

ii. the COLDCARD is *"ultra-secure"* (October 2021-July 2026);

iii. *the COLDCARD uses "dual secure elements," such that "two independent secure-element vendors protect the seed, so one chip flaw is not enough"* (July 2026 - Present);

iv. *the COLDCARD is "the smartest way to secure your Bitcoin"* (from November 2021 - Present);

b. **On the COLDCARD X account:**

i. *users can "sleep like a baby knowing your Bitcoin is secured with COLDCARD"* (July 2026);

ii. *the COLDCARD is "built for serious security"* (April 2026);

iii. *the COLDCARD's "multisig and offline signing ensure your assets are protected from hacks, while encrypted backups and dual secure elements keep your keys safe."* (May 2025).

c. NVK and Coinkite also published the *Bitcoin Security Guide*, which represented COLDCARD's functionality and security features as including Seed Phrase generation and randomness. In particular, the *Guide* represented that cold storage *"Eliminates all remote attack vectors — hackers cannot reach offline keys"*. In the context of promoting COLDCARD, this statement represented to consumers that COLDCARD protected them against remote attacks.

76. Each of these representations was false, misleading or deceptive within the meaning of s. 14 of the *CPA*, because:

a. the COLDCARDs lacked the security-related performance characteristics, benefits or qualities the Defendants represented they possessed (s. 14(2), para. 1);

b. the COLDCARDs did not meet the standards or quality of security represented by the

Defendants (s. 14(2), para. 3);

c. to the extent that the Defendants represented that the COLDCARDs had been supplied in accordance with their previous representations about security, those representations were false because the devices contained the Defect (s. 14(2), para. 7); and

d. the Defendants exaggerated the effectiveness of the COLDCARDs' security features and failed to disclose the Defect, a material vulnerability that caused the devices to generate predictable Seed Phrases, enabling attackers to reconstruct those phrases and steal users' Bitcoin. These exaggerations and omissions deceived or tended to deceive the Plaintiff and Class Members (s. 14(2), para. 14).

77. The Plaintiff and Class Members entered into consumer agreements after or while the Defendants were engaged in unfair practices contrary to the *CPA.* They claim recission and/or damages under s. 18 of the *CPA*, including damages arising from the theft of the Bitcoin that the COLDCARDs were intended to secure.

78. The Plaintiff also requests an order under s. 18(15) of the *CPA* dispensing with any applicable notice requirements. Such an order would be in the interest of justice, having regard to the nature of the Defendants' unfair practices, the losses suffered by the Plaintiff and Class Members, and the impracticability of requiring individual notice.

Negligence

79. Further or in the alternative, the Plaintiff and Class Members claim against the Defendants in negligence.

80. The Defendants owed them a duty of care in the design, development, manufacture, testing, sale and support of the COLDCARD. The Defendants breached the standard of care of a

reasonably prudent designer and seller of dedicated Bitcoin-security hardware, including by failing to warn of the Defect, and thereby caused the Plaintiff and Class Members to suffer the theft and permanent loss of their Bitcoin, as particularized below.

Duty of Care

81. The Defendants owed the Plaintiff and Class Members a duty to exercise reasonable care in respect of the COLDCARD wallet, that required the Defendants, among other things, to:

    a. exercise reasonable skill and care in researching, developing, designing, manufacturing, testing, distributing, selling and marketing the COLDCARD;

    b. verify, through reasonable testing and code review, that the COLDCARD's Seed Phrase generation process used the hardware random-number generator as designed and represented;

    c. exercise reasonable care in designing and implementing the Seed Phrase generation process to produce sufficiently random and unpredictable Seed Phrases to protect users' Bitcoin, consistent with the Defendants' representations;

    d. take reasonable steps to detect and correct the Defect before distributing or selling affected COLDCARDs;

    e. establish and maintain reasonable procedures for identifying, investigating and responding to security defects and breaches, including containing their effects, promptly notifying affected users and mitigating the risk of loss of users' Bitcoin;

    f. reasonably audit, monitor, test and evaluate the COLDCARD's firmware and software, including the firmware containing the Defect;

    g. take reasonable steps to ensure that COLDCARDs were secure, fit for their intended purpose and met the security standards represented by the Defendants;

h. investigate credible reports of security vulnerabilities affecting the COLDCARD, including the report made in or about May 2025, and respond reasonably and promptly;

i. exercise reasonable care to provide accurate and complete information about the COLDCARD's security, including its material limitations and known vulnerabilities;

j. reasonably train and supervise employees and agents responsible for the COLDCARD's design, development, manufacture, testing, auditing and security; and

k. upon discovering, or when they reasonably ought to have discovered, the Defect, promptly investigate it, warn affected users of the associated risks and available protective measures, and take reasonable steps to remedy the Defect and mitigate resulting losses.

82. The Defendants were in a relationship of sufficient proximity with the Plaintiff and the Class Members to owe them a duty of care. The Defendants designed and supplied the COLDCARD and the firmware on which its security depended, sold it directly to the Class Members, made representations about its security on which those Class Members relied, and knew that the Defect was latent and not apparent to an ordinary purchaser through the ordinary use of the device, such that purchasers depended on the Defendants to design and manufacture the COLDCARD in accordance with those representations.

83. There are no policy considerations that would negate the duty of care.

Standard of Care

84. The standard of care required of the Defendants was that of a reasonably prudent designer, manufacturer and seller of dedicated Bitcoin security hardware in the circumstances.

85. The care required was commensurate with the foreseeable likelihood and gravity of harm arising from inadequate security, including the risk that a failure to generate sufficiently random and unpredictable Seed Phrases would expose users to the theft and permanent loss of their Bitcoin.

86. The standard of care was informed by, among other things:

    a. the COLDCARD's intended purpose of securing users' Bitcoin, including through the generation of secure Seed Phrases;

    b. the Defendants' public representations, particularized above, concerning the COLDCARD's security features and the safeguards they represented they had implemented;

    c. prevailing industry standards and practices concerning the security of Bitcoin hardware wallets, including the design and verification of seed-generation processes and the testing, review and auditing of firmware;

    d. the knowledge of Bitcoin security risks that the Defendants possessed or reasonably ought to have possessed at all material times;

    e. the specialized knowledge, skill and expertise the Defendants held themselves out as possessing, including Coinkite's representation that it is *"a leader in Bitcoin security and hardware"*; and

    f. the availability, feasibility and burden of reasonable precautions to prevent or mitigate the foreseeable harm.

87. To meet that standard, the Defendants were required to exercise reasonable skill, care and diligence in designing, manufacturing, testing, updating and supporting the COLDCARD. In particular, they were required to:

a. competently design, implement and verify the COLDCARD's seed-generation process, including the generation, processing and use of sufficient cryptographic entropy;

b. verify, through appropriate testing of the implemented firmware, that the seed-generation process actually used the intended cryptographically secure sources of randomness and did not substitute an insecure software generator;

c. conduct reasonable security testing, code review and auditing of the COLDCARD's firmware, including before releasing firmware to users, to identify defects that could compromise seed generation or security;

d. investigate and take reasonable and timely action in response to credible reports that the COLDCARD's security was or might be compromised; and

e. upon discovering, or when they reasonably ought to have discovered, the Defect, promptly warn affected users of the associated risks and available protective measures, and take reasonable steps to remedy the Defect and prevent or mitigate resulting losses.

88. The Defendants breached the applicable standard of care, as particularized below.

The Breaches – Negligent Design and Failure to Warn

89. The Defendants breached their duty of care in two respects: (i) by failing to prevent or detect the Defect in the design and implementation of the COLDCARD; and (ii) by failing to warn users of the Defect and its associated risks.

90. **Negligent Design**: the Defendants negligently designed, manufactured, and supplied the COLDCARD and its firmware, in that they:

a. designed and implemented the COLDCARD's seed generation with the Defect in

place;

b. failed to verify, through reasonable testing or audits, that the COLDCARD in fact generated its Seed Phrase using sufficiently random methods;

c. were aware or ought to have been of the Defect, and nevertheless introduced defective COLDCARD wallets to the market;

d. failed to detect or correct the Defect for more than five years, despite reasonable opportunities to do so and specific warnings of the Defect's existence; and,

e. supplied COLDCARDs preloaded with, or updated to, the Defect, thereby supplying consumers with a device that was not secure, not fit for its intended purpose, and did not perform as represented.

91. **Failure to Warn**: the Defendants failed to provide timely and adequate warnings to the Plaintiff and Class Members, in that they:

a. knew, or ought to have known, of the Defect from at least May 2025, yet failed to alert COLDCARD owners and users of the Defect and the risk it posed to their Bitcoin;

b. failed to promptly notify affected COLDCARD owners when unauthorized transfers began on or about July 30, 2026, despite possessing customer contact information;

c. failed to take reasonable steps to reach all affected owners, including those who purchased their devices through resellers or whose contact information was outdated or unavailable;

d. failed to provide sufficiently clear, prominent and urgent warnings explaining that the Defect exposed existing Seed Phrases, that updating the firmware alone would

not protect their Bitcoin, and that immediate migration to new Seed Phrases was necessary;

e. initially advised owners of newer COLDCARD models that their devices were unaffected, thereby misleading affected owners about the risk to their Bitcoin;

f. failed to take reasonable steps to ensure that owners could distinguish legitimate security warnings from fraudulent communications and phishing attempts; and

g. failed to establish and implement an adequate response plan or notification protocol for foreseeable security defects, vulnerabilities and breaches.

Causation

92. The Defendants' negligence caused the loss and damage suffered by the Plaintiff and the Class Members, particularized below. But for the Defendants' breaches of their duty and standard of care, the Plaintiff and the Class Members would not have lost their Bitcoin.

93. That loss followed directly from the Defect. Because the COLDCARD generated predictable Seed Phrases, attackers were able to reproduce those Seed Phrases, derive the corresponding private keys, and transfer the Plaintiff's and the Class Members' Bitcoin without their knowledge or authorization. Had the COLDCARD generated Seed Phrases with the randomness the Defendants represented, the Plaintiff's and the Class Members' Bitcoin could not have been taken in this way.

94. That loss was therefore a reasonably foreseeable consequence of the Defendants' negligence and was not too remote. Theft of Bitcoin through the reproduction of predictable Seed Phrases was the precise risk the COLDCARD was designed and marketed to prevent.

95. The risk was known to the Defendants. NVK recognized it in the newsletter described at paragraph 62 above, and the Defendants had actual notice of the Defect from at least May

2025. The Defendants knew, or ought to have known, that defective Seed Phrase generation would expose owners to the theft of their Bitcoin. The thefts were the realization of the very risk that made the Defendants' conduct negligent.

Negligent Misrepresentation

96. Further or in the alternative, the Defendants' representations particularized in paragraphs 73–76 above, particularly that COLDCARD securely generated random Seed Phrases that no one else could reproduce, were negligent misrepresentations. They were untrue, inaccurate and misleading.

97. The Defendants owed the Plaintiff and Class Members a duty of care arising from a special relationship because:

    a. the Defendants undertook to provide accurate information about COLDCARD's security, knowing and intending that purchasers would rely on their representations in deciding to purchase and use the device to secure their Bitcoin; and

    b. such reliance was reasonable and reasonably foreseeable. The Defendants held themselves out as possessing specialized knowledge and expertise in Bitcoin security. They made the representations deliberately, in marketing, online and product materials, in the course of their business and for their financial benefit. The representations concerned COLDCARD's central security function, which ordinary purchasers could not independently verify.

98. The representations were directed to a defined and ascertainable class, purchasers and users of COLDCARD, for the specific purpose of inducing them to purchase and use the device to secure their Bitcoin.

99. The Defendants made the representations negligently. They knew or ought to have known

that the representations were untrue or misleading and failed to take reasonable care to ensure their accuracy, including by failing to verify that COLDCARD generated Seed Phrases with sufficient randomness and by continuing to make the representations after learning of the Defect in or about May 2025.

100. The Plaintiff and Class Members reasonably relied on the representations for the very purpose for which Coinkite made them. In reliance on the representations, they:

a. purchased COLDCARD devices and paid the purchase price;

b. generated and used Seed Phrases produced by COLDCARD to secure their Bitcoin rather than adopting alternative wallets, custody methods or security measures; and

c. continued to rely on those Seed Phrases instead of taking steps to protect their Bitcoin.

101. The Plaintiff and Class Members relied on the representations to their detriment. But for the representations:

a. they would not have purchased or used the affected COLDCARD devices to secure their Bitcoin, or continued relying on vulnerable Seed Phrases; and

b. they would have adopted alternative security measures and avoided the theft of their Bitcoin and the resulting losses.

Breach of the Sale of Goods Act, R.S.O. 1990, c. S.1;

102. Further or in the alternative, the Class Members are *"buyers"* and the Defendants are *"sellers"* within the meaning of s. 1 of the *SGA*. The COLDCARDs are *"goods"* within the meaning of s. 1.

103. The parties entered into a *"contract of sale of goods"* within the meaning of s. 2 of the *SGA*.

104. The Defendants sold the COLDCARD by description as a Bitcoin hardware wallet that securely generates a random Seed Phrase no other person can reproduce. There was an implied condition under s. 14 of the *SGA* that the goods would correspond with the description. Because of the Defect, the COLDCARD did not correspond to that description.

105. The COLDCARD has a single purpose: the secure self-custody of Bitcoin. By purchasing the COLDCARD, the Class Members impliedly made that purpose known to the Defendants and relied on the Defendants' skill and judgment to supply a device fit for that purpose.

106. Only the Defendants were in a position to ensure that the device generated a secure, random Seed Phrase. Accordingly, there was an implied condition that the COLDCARD would be reasonably fit for that purpose pursuant to s. 15 para. 1 of the *SGA*. Because of the Defect, it was not.

107. The Plaintiff and Class Members bought the COLDCARD by description from Defendants, a seller who deals in goods of that description. Accordingly, there was an implied condition that it would be of merchantable quality under s. 15, para. 2 of the *SGA*. Because of the Defect, it was not. The Defect was latent and was not a defect that any examination by the Class Members could or ought to have revealed.

108. The Class Members accepted the COLDCARDs within the meaning of s. 34 of the *SGA*. Pursuant to *SGA* s. 12(3), the Class Members treated and are treating the breaches of the foregoing implied conditions as breaches of warranty. The Class Members claim damages under s. 51 of the *SGA,* as particularized below.

Breach of Contract

109. Further or in the alternative, the Plaintiff and the Class Members claim against Coinkite for breach of contract.

110. Each Class Member entered into a binding contract with Coinkite for the supply, setup, and operation of a COLDCARD device and its accompanying operating firmware:

a. directly, by purchasing the device from Coinkite through its website or sales channels and paying the purchase price; and/or

b. through collateral contracts and warranties arising from Coinkite's representations and undertakings made directly to end users who acquired COLDCARD devices through authorized third-party retailers, distributors, or resellers, including representations concerning device security, cryptographic entropy, and firmware integrity, upon which those purchasers relied in purchasing, initializing, and using the devices.

111. It was an express or implied term of these contracts, including any collateral warranties, that:

a. the COLDCARD would possess and maintain the security features Coinkite represented and marketed, including the generation of cryptographically secure, random, and unpredictable Seed Phrases derived from an unbiased hardware random number generator;

b. the COLDCARD would be reasonably fit for its intended purpose of securely generating, isolating, and protecting the private keys controlling access to Class Members' Bitcoin;

c. the COLDCARD would be of acceptable and merchantable quality, durable, and free from defects that materially compromise its cryptographic security; and

d. all firmware supplied, updated, or deployed by Coinkite would preserve the integrity of the seed-generation process and would not weaken, degrade, or compromise the entropy or security of Seed Phrases generated on the device.

112. Coinkite breached each of these terms. Because of the Defect:

a. the COLDCARD generated Seed Phrases with defective and degraded cryptographic randomness, enabling unauthorized third parties to regenerate or predict private keys offline and access the associated Bitcoin;

b. the COLDCARD lacked the essential security features Coinkite represented and marketed;

c. the COLDCARD was not reasonably fit for its intended purpose of securely storing and protecting private keys controlling access to Class Members' Bitcoin; and

d. the COLDCARD was not of acceptable or merchantable quality, was inherently vulnerable upon setup, and was commercially worthless for its intended purpose.

113. These breaches went to the root of the contracts and deprived the Plaintiff and the Class Members of substantially the whole benefit of their bargain. The essential purpose and function of the COLDCARD was to safeguard private keys controlling access to Bitcoin. The Defect defeated that essential purpose.

114. To the extent Coinkite relies on any contractual exclusion, disclaimer, arbitration agreement, or limitation of liability in its terms of sale or end user agreements, the Plaintiff and the Class Members plead that:

a. pursuant to s. 7(1) of the *CPA*, the substantive and procedural rights under the *CPA* apply despite any agreement or waiver to the contrary. These include the *SGA* implied conditions, which s. 9(2) deems to apply to consumer agreements. Pursuant to *CPA* s. 9(3), any term purporting to negate or vary those implied conditions is void. Pursuant to *CPA* ss. 7 and 8(1), any term requiring arbitration, or preventing the Class Members from commencing or participating in a class proceeding, is invalid;

b. properly construed, the provision does not apply to or exclude liability for the fundamental failures and breaches alleged;

c. the provision is unconscionable, harsh, and unenforceable at the time of contract formation; and/or

d. the Court should refuse enforcement of the provision on the grounds of overriding public policy pursuant to the framework in *Tercon Contractors Ltd. v. British Columbia (Transportation and Highways)*, 2010 SCC 4.

115. As a direct, proximate, and foreseeable result of Coinkite's breaches, the Plaintiff and the Class Members suffered loss and damage as particularized below.

116. The parties reasonably contemplated these losses at the time of contracting as the probable and natural result of a breach. Coinkite knew that purchasers relied entirely on the COLDCARD's entropy mechanisms to secure their Bitcoin, that defective seed generation would expose those funds to unauthorized derivation and theft, and that purchasers would incur necessary expenses to mitigate the Defect and protect their remaining assets.

Personal Liability of NVK and Gray

117. The Plaintiff claims against the Defendants NVK and Gray personally.

118. NVK and Gray each owed the Plaintiff and the Class Members a duty of care independent of their positions at Coinkite.

119. NVK and Gray each personally committed the acts and omissions described below, which were tortious in themselves and went beyond the ordinary direction of Coinkite's affairs.

120. **As against NVK**: he is personally liable to the Plaintiff and the Class Members in negligence and negligent misrepresentation, and under the *CPA* and *SGA* for his own acts and omissions, independently of his position as Coinkite's co-founder, director, and Chief Executive Officer.

121. NVK personally cultivated a position of trust and expertise in Bitcoin security and made authoritative representations under his own name, including in his 2023 *Bitcoin Security Guide* referred to above and through his social-media account (@nvk). Through these representations, NVK personally vouched for the COLDCARD's cryptographic security, including the integrity of its seed-generation process, intending or reasonably expecting purchasers and users, including the Plaintiff and Class Members, to rely on those assurances.

122. NVK knew, no later than January 20, 2023, that inadequate entropy in seed generation could compromise users' private keys and expose their Bitcoin to theft. Despite that knowledge, he continued personally to represent the COLDCARD as cryptographically secure without taking reasonable steps to verify the accuracy of those representations.

123. NVK knew or ought to have known whether those assurances were true. He failed to investigate and correct the Defect when it became or ought to have become apparent, and failed to correct his representations or warn users of the resulting danger.

124. The Plaintiff and Class Members reasonably relied on NVK's representations in acquiring or continuing to use affected COLDCARD devices and recovery phrases.

125. By his personal misrepresentations and omissions, NVK induced or contributed to users' continued reliance on compromised cryptographic credentials, thereby causing or contributing to the theft of their Bitcoin and their resulting losses.

126. **As against Gray**: he is personally liable to the Plaintiff and the Class Members in negligence and negligent misrepresentation, and under the *CPA* and *SGA* for his own acts and omissions, independently of his position as Coinkite's Chief Technology Officer.

127. Gray personally designed, developed, and implemented the COLDCARD's cryptographic architecture and seed generation software, including the Defect. He personally participated in introducing the Defect into production firmware, deploying it, and permitting its continued distribution.

128. After receiving the May 2025 warning about the Defect noted above, Gray personally dismissed it without adequately investigating the vulnerability, correcting the Defect, or warning users of the risk. Despite knowing, or having reason to know, that the Defect — his Defect — could expose users' Bitcoin to theft, Gray permitted the affected firmware to remain in use without adequate remediation or notice.

129. Gray knew or ought to have known that Class Members relied on the COLDCARD's cryptographic security to protect their assets and that defective seed generation exposed them to a foreseeable risk of theft.

130. By personally undertaking responsibility for the design, development, implementation, and security of the seed-generation software, and by personally receiving and dismissing a specific warning of its vulnerability, Gray owed the Class Members a duty to exercise

reasonable care in performing those functions, including investigating, correcting, and warning of known security defects.

131. Gray breached that duty through his own negligent acts and omissions, which caused or materially contributed to the theft of the Class Members' Bitcoin and their resulting losses.

132. **As against both NVK and Gray**: By reason of the matters pleaded above, NVK and Gray each personally owed, and breached, the duty and standard of care pleaded in the Negligence section of this Claim. Those personal breaches caused the loss and damage suffered by the Plaintiff and the Class Members, particularized below.

133. NVK and Gray are each personally liable for that loss and damage, jointly and severally with Coinkite and with each other.

Piercing the Corporate Veil

134. Further, or in the alternative, the Plaintiff and the Class Members plead that Coinkite's separate corporate personality should be disregarded and that NVK and Gray should be held personally, jointly and severally liable with Coinkite for the losses and damages arising from the wrongful conduct alleged in this Claim.

135. At all material times, NVK and Gray exercised complete domination and control over Coinkite and its affairs. In particular:

a. NVK and Gray founded Coinkite, were its directing minds, and controlled its management, business strategy and operations;

b. Gray, as Coinkite's Chief Technology Officer and co-founder, directed and participated in the development, maintenance and deployment of COLDCARD firmware, including its cryptographic security and seed-generation systems;

c. Gray personally contributed to the development and maintenance of software incorporated into COLDCARD firmware, including components associated with the seed-generation process implicated in the Defect;

d. NVK and Gray controlled Coinkite's decisions concerning the design, manufacture, marketing and distribution of COLDCARD devices and their advertised security features;

e. NVK and Gray controlled Coinkite's decisions concerning firmware development, testing, approval, release and remediation, including its response to security vulnerabilities; and

f. NVK and Gray controlled Coinkite's public representations concerning COLDCARD security and its communications with users concerning the Defect and the resulting risks to their Bitcoin.

136. NVK and Gray used their domination and control of Coinkite to direct and carry out the wrongful conduct particularized above through the corporation, including:

a. directing the development, approval and distribution of COLDCARD firmware containing the Defect without adequate verification or testing of its cryptographic seed-generation process;

b. directing the continued marketing and sale of COLDCARD devices as secure hardware wallets when they knew, or were wilfully blind to the Defect;

c. authorizing and maintaining representations concerning the COLDCARD's cryptographic security and its generation of random and unpredictable Seed Phrases when they knew, or were wilfully blind as to whether, those representations were false or misleading;

d. concealing the Defect and withholding warnings of the resulting risk to users' Bitcoin after becoming aware of the vulnerability; and

e. controlling Coinkite's response to the unauthorized transfers of Bitcoin from July 30, 2026, including the timing, content and adequacy of its security warnings and remedial measures.

137. NVK and Gray used Coinkite as the instrument through which they directed and carried out this improper conduct. They completely dominated Coinkite, which did not exercise independent judgment or control in the matters giving rise to the Plaintiff's and Class Members' claims. The wrongful conduct carried out through Coinkite caused the losses and damages claimed.

138. Accordingly, the Plaintiff and the Class Members plead that Coinkite's separate corporate personality should be disregarded and that NVK and Gray should be held personally, jointly and severally liable with Coinkite for the losses and damages arising from that conduct.

Damages

139. As a result of the Defendants' breaches of contract, statutory breaches, negligence and other wrongful acts and omissions pleaded above, the Plaintiff and the Class Members suffered loss and damage, including:

a. **Loss of Bitcoin:** the value of Bitcoin stolen through unauthorized transfers resulting from the Defect, assessed at the date of theft, the date of judgment, the highest intermediate market value where legally recoverable, or such other date as the Court determines will properly compensate the Plaintiff and the Class Members for their losses. Alternatively, the Plaintiff and Class Members claim restoration of the

quantities of Bitcoin stolen by delivering equivalent quantities to secure wallets designated by them.

b. **Lost Investment Income and Opportunities:** lost investment income, profits, appreciation and other returns, including identifiable opportunities to hold, trade, lend, pledge as collateral or otherwise use the stolen Bitcoin.

c. **Defective Devices:** the purchase price, shipping costs, customs duties and import fees paid for the defective COLDCARD devices, and/or their diminution in value, including any total loss of value.

d. **Mitigation and Replacement Costs:** reasonable expenses incurred to protect remaining Bitcoin and replace or secure compromised wallets, including replacement hardware wallets, signing devices, backup equipment, security hardware and related technical services;

e. **Transaction Fees:** blockchain network fees, expedited transaction fees and other costs incurred in transferring Bitcoin to secure wallets or replacing stolen Bitcoin;

f. **Exchange and Conversion Costs:** trading spreads, commissions, conversion charges, exchange fees and other expenses reasonably incurred in replacing stolen Bitcoin or restoring liquidity;

g. **Business Interruption:** lost business profits, additional operating expenses and other commercial losses arising from the inability to access or use stolen Bitcoin as working capital or a means of payment;

h. **Financing Costs:** interest, borrowing costs, loan fees and other financing costs reasonably incurred to replace stolen Bitcoin, maintain credit facilities or meet financial obligations;

i. **Forced Asset Sales:** losses from the forced or premature sale of other investments or assets to replace stolen Bitcoin or meet financial obligations;

j. **Tax and Accounting Expenses:** additional tax liabilities, accounting expenses and other tax-related costs arising from the theft, mitigation measures or replacement transactions, including expenses incurred in determining, documenting and reporting the resulting tax consequences and reconstructing adjusted cost bases; and

k. **Other Consequential Losses:** such further financial losses, incidental expenses and reasonable out-of-pocket costs as resulted from the Defect and the resulting thefts.

140. The Plaintiff and the Class Members claim compensation for the foregoing loss and damage.

141. The loss and damage were reasonably foreseeable consequences of the Defendants' wrongful conduct and, in respect of the contractual claims, were within the reasonable contemplation of the contracting parties when their contracts were formed.

142. The Plaintiff and the Class Members claim general and special damages, without double recovery. Further particulars of special damages will be provided as they become known, in accordance with the *Rules of Civil Procedure*, including through any individual claims process ordered under the *Class Proceedings Act, 1992*.

Punitive and Aggravated Damages

143. The Plaintiff and the Class Members claim punitive damages. The Defendants' conduct was high-handed, malicious and reprehensible, and departed markedly from the standards of conduct expected of them.

144. The Defendants knew, or were wilfully blind to the fact, at least a year before the

unauthorized transfers began, that the COLDCARD suffered from serious deficiencies in its cryptographic seed-generation process. Nevertheless, they continued to market and sell the COLDCARD as secure, maintained misleading representations concerning its security, and concealed the Defect and the resulting risks from purchasers. They placed their commercial interests ahead of the security of the assets entrusted to their products. Their conduct warrants an award of punitive damages to punish and denounce their misconduct and deter similar conduct, because compensatory and aggravated damages alone would be insufficient to achieve those purposes.

145. The Plaintiff and the Class Members also claim aggravated damages. The Defendants' misrepresentations concerning the COLDCARD's security, and their concealment of the Defect and the resulting risk to users' Bitcoin, aggravated the harm suffered by the Plaintiff and Class Members whose Bitcoin was stolen. Their conduct caused additional mental distress, anxiety, humiliation and loss of peace of mind beyond the distress arising from the financial losses themselves.

146. This action is materially tied to Toronto as the COLDCARD wallets are produced and manufactured in Toronto.

RELEVANT STATUTES

147. The Plaintiffs and the Class Members plead and rely upon, and the amendments made thereto and the regulations thereunder and the Provincial equivalents:

a. *Class Proceedings Act*, 1992, S.O. 1992, c. 6;

b. *Courts of Justice Act*, R.S.O. 1990, c. C.43;

c. *Consumer Protection Act, 2002*, S.O. 2002, c. 30;

d. *Sale of Goods Act*, R.S.O. 1990, c. S.1; and

e. *Negligence Act*, R.S.O. 1990, c. N.1.

148. The Plaintiff proposes that this action be tried at Toronto, Ontario.

DIAMOND & DIAMOND LAWYERS LLP
500-255 Consumers Road
Toronto, ON M2J 1R4
T:(416) 256-1600

Darryl Singer
LSO no. 34473R
darryl@diamondlaw.ca

Mathura Santhirasegaram
LSO no. 73033G
mathura@diamondlaw.ca

Shir Zisckind
LSO no. 89950M
shir@diamondlaw.ca
Lawyers for the Plaintiff

BENEDETT
Plaintiff

- and -

COINKITE INC et al
Defendants
Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE
Proceeding Commenced at Toronto

STATEMENT OF CLAIM

DIAMOND & DIAMOND LAWYERS LLP
500-255 Consumers Road
Toronto, ON M2J 1R4

Darryl Singer (34473R)
T: (416) 256-1600
darryl@diamondlaw.ca

Mathura Santhirasegaram (73033G)
mathura@diamondlaw.ca

Shir Ziskind (89950M)
shir@diamondlaw.ca

Lawyers for the Plaintiff