IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Xu v. NDAX Canada,*
2025 BCSC 2048

Date: 20251020
Docket: S246940
Registry: Victoria

Between:

Yan Li Xu

Plaintiff

And:

NDAX Canada

Defendant

Before: The Honourable Justice LeBlanc

Reasons for Judgment

The Plaintiff, appearing in person:	Y. Xu
Counsel for the Defendant:	L. Hale R. Kelba
Place and Dates of Trial:	Victoria, B.C. September 22–24, 2025
Place and Date of Judgment:	Victoria, B.C. October 20, 2025

INTRODUCTION

[1] If an investment proposal sounds too good to be true, it probably is. That was the case for the plaintiff who found herself to be the unfortunate victim of a cryptocurrency scam.

[2] While I found the plaintiff's losses are regrettable, I have found no liability rests with the defendant in this action, a crypto assets trading platform, registered as a money service business with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"). The defendant identified suspicious financial activity and cautioned the plaintiff not to proceed. Unfortunately, the plaintiff did not heed the warning.

FINDINGS OF FACT

[3] The plaintiff testified that she was befriended by someone she cannot name. This person initially convinced the plaintiff to send him relatively small amounts ($500 and $1,000). These initial small investments were returned to the plaintiff along with generous returns. After the plaintiff's trust was established, the plaintiff was asked to purchase a large sum of cryptocurrency on the promise that if invested she would make a significant return in the range of 1% per day.

[4] To purchase the cryptocurrency, the plaintiff remortgaged her house and borrowed money from a friend.

[5] On April 10, 2023, the plaintiff opened an account with NDAX (the "Account") through their online platform. To satisfy FINTRAC compliance requirements, the defendant required the plaintiff to provide, as part of the Account opening process, her personal information and government issued identification, which was verified by the defendant.

[6] On opening the Account, the plaintiff was presented with a User Agreement and separate Risk Statement for review and acceptance. The plaintiff did not read the User Agreement or the Risk Statement and clicked on the "accept" button so that she could open the Account. By clicking accept, the plaintiff agreed she received,

read and understood the Risk Statement and agreed to the terms of the User Agreement.

[7] After opening the Account, the plaintiff made multiple deposits of Canadian dollars. Between April 11, 2023 and May 17, 2023, the plaintiff deposited $671,000 (the "Funds") into the Account. The plaintiff used the Funds to purchase units of Ethereum, a cryptocurrency.

[8] On April 18, 2023, the plaintiff initiated a withdrawal of Ethereum to an external wallet (the "First Withdrawal"). To facilitate the transfer, the plaintiff provided a personal wallet address to the defendant.

[9] When it received the plaintiff's request to process the First Withdrawal, the defendant provided the plaintiff with a number of warnings and disclosures concerning the risk associated with continuing.

[10] First, the plaintiff was provided with a withdrawal crypto risk disclosure statement (the "Crypto Risk Disclosure") which read as follows:

> Sending cryptocurrency to an untrusted wallet can result in the permanent loss of your funds. To protect yourself, please take the following precautions:
>
> - Do not proceed with this withdrawal if anyone has accessed your device remotely.
> - Only send cryptocurrency to trusted wallets.
> - Be wary of unsolicited messages offering free cryptocurrency or lucrative investment opportunities.
> - Verify the authenticity of any website, wallet, or trading platform/exchange before sending cryptocurrency.
> - Beware of scammers posing as legitimate businesses, government employees, or representatives of regulatory bodies. Note that these individuals will never ask for your login credentials or request that you send them cryptocurrency.
> - Only engage in transactions that you fully understand.
> - Beware of common cryptocurrency scams, such as high-return investments, Ponzi schemes, social engineering, take giveaways, and take ISO's
>
> Learn More [Link]
>
> If you have any concerns about the safety and security of your cryptocurrency transactions or believe you may have been a victim of a scam or fraud, please contact us immediately at [indiscernible due to quality of photocopy].

[11] The plaintiff confirmed to the defendant that she had received and understood the Crypto Risk Disclosure by clicking accept on these platform pages.

[12] Second, the plaintiff received the following secondary disclosure (the "Second Warning") and confirmed to the defendant that she wanted to continue:

> I confirm the information I've provided is accurate, correct, and complete. I understand crypto asset withdrawals are final and irreversible. NDAX will not be liable for losses from my inaccurate information or for delays from network issues outside NDAX's control.

[13] Third, the plaintiff was contacted by an employee of the defendant on April 18, 2023 seeking further information on the transaction and warning the plaintiff that she is likely "being scammed" and should not proceed with the transaction (the "Third Warning"). The plaintiff continued to advise the employee that she wished to proceed. The plaintiff was advised that the call would be escalated as the transaction exhibited risk factors. The telephone call was recorded (the "Recording"). I find that the defendant's warnings to the plaintiff could not have been clearer.

[14] Following this call, the plaintiff sent a number of emails to the defendant demanding they proceed with the withdrawal without delay. The plaintiff's tone escalated to where she was threatening legal action against the defendant if they did not proceed.

[15] Fourth, the plaintiff was contacted by Julia Baranovskaya, a compliance officer with the defendant (the "Fourth Warning"). The purpose of the call was to confirm the plaintiff understood the risks associated with proceeding with the First Withdrawal and confirm the plaintiff's instructions to proceed. During the call, the plaintiff was (a) informed of the risks of trading in cryptocurrency; (b) that she might be the target of cryptocurrency fraud; and (c) advised that once the First Transaction is processed, it would be irreversible. The plaintiff confirmed to Ms. Baranovskaya that (a) she knew what she was doing and that no one controls her; (b) that she has been trading stocks for over 20 years and understood the risks associated with trading in cryptocurrency; (c) that she is an accountant by trade and reaffirmed her understanding of the risks; (d) that the source of the Funds was her investment

savings that she was reinvesting; and (e) that she was aware that if the First Transaction was processed it could not be recovered from the recipient wallet. The plaintiff confirmed her instructions for the defendant to process the First Transaction and the defendant followed the instructions.

[16] Following the First Transaction, the plaintiff proceeded with two additional transfers to the same recipient wallet. During these transfers, the plaintiff was provided with and approved the Crypto Risk Disclosure and the Second Warning.

[17] Despite the warnings, the plaintiff transferred all of the purchased Ethereum to a cryptocurrency wallet controlled by a third party becoming the victim of a cryptocurrency scam, resulting in the loss of the Funds.

[18] Prior to processing the First Transaction, the defendant conducted a BitRank analysis on the recipient wallet and it received a score of 54 which was within the acceptable limits to process the transfer. Ms. Baranovskaya explained that when a wallet is opened it receives a score of 50 and the score will go down if there is suspicious activity and up for trusted activity with 50 and above being acceptable and under 50 as unacceptable. If a wallet is flagged for fraudulent activity it would receive a score of zero. Ms. Baranovskaya further explained that based on the BitRank score there was no reason not to process the transaction following the warnings provided to the plaintiff and on receiving the instructions from the plaintiff to proceed. This evidence went unchallenged under cross-examination.

[19] Ms. Baranovskaya testified that the defendant did not know who controlled the recipient wallet as that information was not known to the defendant and all they could do was warn the plaintiff that the First Transaction exhibited signs of potential fraud. This evidence was also unchallenged.

[20] The plaintiff asserts the Recording is not a true recording although agreed it was her voice on the Recording. The employee that provided the Third Warning and Ms. Baranovskaya both testified that the Recording was unaltered and represented a complete version of the telephone call with the plaintiff. The plaintiff testified that

certain portions of the call had been removed although she could not identify which portions she claimed had been deleted.

[21] I found the defendant's witnesses credible and have no reason to conclude that the Recording is not a true and complete representation. Further, the plaintiff did not refute the warnings contained on the Recording occurred and those clearly provided that she was potentially at risk.

APPLICABLE LEGAL PRINCIPLES

[22] The plaintiff asserts that the defendant breached a duty of care that was owed to her. The plaintiff says that the defendant ought to have advised her that the recipient wallet was a "scammer".

[23] As held by the Supreme Court of Canada, a duty of care is established by the conjunction of the proximity of relationship and foreseeability of injury: *1688782 Ontario Inc. v. Maple Leaf Foods Inc.,* 2020 SCC 35 [*Maple Leaf*] at para. 30.

[24] To be successful in a claim for negligence, a plaintiff must establish that: (a) a duty of care was owed by the defendant; (b) the defendant's conduct fell below the standard related to the duty of care; (c) the plaintiff sustained damages; and (d) the damages were caused, in fact and in law, by the defendant's breach of the duty of care: *Maple Leaf* at para. 18.

[25] Where a defendant undertakes to provide a service to a plaintiff in a manner that invites reliance, the defendant has a duty to provide reasonable care: *Maple Leaf* at para. 32.

[26] A bank owes its customers a duty to exercise reasonable care and skill in discharging its obligations to a customer: *Groves-Raffin Construction Ltd. v. Bank of Nova Scotia*, [1976] 64 D.L.R. (3d) 78 at 83, 1975 CanLII 912 (B.C.C.A.) ["*Groves-Raffin*"]. This duty is based on ordinary banking practices situated within the context of the relationship between the bank and its customer and the nature of the transaction: *Groves-Raffin* at 121; *Foodinvest Limited v. Royal Bank of Canada,*

2018 ONSC 7742 at para. 10, aff'd *Foodinvest Limited v. Royal Bank of Canada* 2020 ONCA 665 ["*Foodinvest*"].

[27] Where there are suspicious or sufficiently unusual circumstances, a bank may have a duty to inquire and warn a customer when they give instructions about a particular transaction: *Zheng v. Bank of China (Canada) Vancouver Richmond Branch,* 2023 BCCA 43 at para. 42.

[28] Suspicious or unusual circumstances may include:

(a) a transfer of money not in line with the purposes of the account or that is of an unusual amount for the particular customer;

(b) the amount of money being transferred in relation to the customer's total account holdings;

(c) the customer's conduct in relation to the transaction; and

(d) the bank's knowledge of any prevailing scams targeting a similar demographic.

Zheng at paras. 38–42.

[29] Each case will turn on its individual facts: *Zheng* at para. 37.

[30] Where a duty of care is found to exist in a relationship between a bank and a customer, the standard of care to be met is that of a "reasonable banker": *Groves-Raffin* at paras. 83–84.

[31] Expert evidence is generally required to determine the standard of care when the nature of the issue cannot be decided based on the ordinary knowledge by the trier of fact: *International Culinary Institute of Canada, Inc. v. Grant Thronton LLP*, 2010 BCSC 541 at paras. 31–32, citing *ter Neuzen v. Korn*, [1995] 3 S.C.R. 674, 1995 CanLII 72 (S.C.C.).

[32] If there is an established breach of the standard of care, the plaintiff must establish factual causation by showing that, on a balance of probabilities, the harm would not have occurred but for the defendant's negligent act: *Revelstoke (City) v. Gelowitz*, 2023 BCCA 139 at para. 62 ["*Revelstoke*"], citing *Nelson (City) v. Marchi*, 2021 SCC 41 at para. 96.

[33] To establish legal causation, a plaintiff must establish that the actual injury was a "foreseeable result of a defendant's negligent conduct": *Revelstoke* at para. 75.

DISCUSSION

[34] To establish where the duty may rest in financial transactions, evidence establishing a reasonable standard is generally required. The plaintiff has not led such evidence in this case. Notwithstanding the lack of evidence establishing what the standard is, I am able to conclude that the defendant satisfied any standard of care that would have been applicable.

[35] The defendant provided as part of its standard practice a routine warning system consisting of the Crypto Risk Disclosure and the Second Warning.

[36] Upon the plaintiff initiating the First Transaction, it recognized a potential financial risk and within the Third Warning and Fourth Warning took steps to specifically warn the plaintiff that she may be the subject of a financial scam and should not proceed. The plaintiff ignored these clear and repeated warnings and insisted that the defendant proceed with the First Transaction.

[37] The plaintiff takes issue with the defendant not warning her that the recipient wallet was held by a scammer. This was information the defendant did not have at the time the First Transaction was initiated. The defendant attempted to obtain further information from the plaintiff to assist her in identifying the recipient wallet and the plaintiff provided false and misleading information in response to the defendant's questions, including advising the defendant that the recipient wallet was owned and controlled by her, which was false. The defendant identified the potential

that the recipient wallet may be held by a scammer and notified the plaintiff of this information. The plaintiff ignored the defendant. There is no evidence or basis to conclude that further warnings by the defendant would have convinced the plaintiff or had any effect beyond the warnings already received.

[38] Upon the plaintiff threatening the defendant with legal action if the First Transaction was not processed, the defendant attempted the Fourth Warning, to convince the plaintiff not to proceed. The plaintiff was insistent that she knew what she was doing and approved processing the First Transaction.

[39] Other than refusing to process the First Transaction, something the defendant was not entitled to do, I find there is nothing further the defendant could have been expected to do to prevent the loss the plaintiff suffered.

[40] The plaintiff continued with subsequent transfers of her cryptocurrency failing to consider the Crypto Risk Disclosure, the Second Warning, the Third Warning or the Fourth Warning, resulting in her loss of the Funds.

[41] The plaintiff has failed to establish that the defendant breached its duty of care and I find that, in any event, the defendant did not cause the losses experienced by the plaintiff.

[42] The defendant raised, as a defence, the scope of the User Agreement and its impact on the nature of the relationship between the parties. With consideration to my findings above, I need not consider that issue.

ORDERS MADE

[43] I dismiss the plaintiff's claim. The defendant is entitled to its costs on Scale B.

"Justice LeBlanc"