KING'S BENCH FOR SASKATCHEWAN

Citation: 2025 SKKB 123

Date: **2025 08 08**
File No.: KBG-SC-00086-2023
Judicial Centre: Swift Current

BETWEEN:

HONEYBADGER ENTERPRISES LTD.

PLAINTIFF

- and -

NORMAN BUE AND INNOVATION CREDIT UNION

DEFENDANTS

Counsel:

Travis Kusch and Jared Epp	for the plaintiff
Jean-Pierre Jordaan	for the defendant Norman Bue
Reid Lester	for the defendant Innovation Credit Union

JUDGMENT
AUGUST 8, 2025

RICHMOND J.

---

[1] An internet fraud has left two innocent victims in its wake. The plaintiff, HoneyBadger Enterprises Ltd. [HoneyBadger], is a corporation in the business of selling cryptocurrency. Mr. Bue is a retiree from Cabri, Saskatchewan. He was 66 at the time the action was commenced. Mr. Bue made contact with HoneyBadger in April 2023 to make inquiries about an over the counter [OTC] purchase of cryptocurrency. At the time, HoneyBadger was completing OTC transactions by either wire transfer from the purchaser sent to HoneyBadger or by way of Pre-Authorized Debit Agreement [PAD Agreement] by which the purchaser provides authorizations for debits from the purchaser's account at a financial institution. Following discussions with a

2025 SKKB 123 (CanLII)

HoneyBadger employee, a PAD Agreement was signed by Mr. Bue authorizing withdrawals by HoneyBadger from his Innovation Credit Union [Credit Union] account. Cryptocurrency was then purchased using the PAD Agreement over the course of several days in the amount of $240,000. The Credit Union, on Mr. Bue's request, cancelled the transactions and had the money returned. As a result, HoneyBadger commenced an action against both Mr. Bue and the Credit Union. HoneyBadger obtained a without notice Order preserving the funds which Order was subsequently confirmed in chambers. Once the funds were preserved, HoneyBadger discontinued its claim against the Credit Union.

[2] HoneyBadger, having transferred cryptocurrency, demands the funds previously withdrawn pursuant to the PAD Agreement as it has not received payment for the cryptocurrency. Mr. Bue, on the other hand, asserts he did not make the purchase of some of the cryptocurrency in question and did not receive the benefit of any cryptocurrency as it was deposited to a wallet operated by fraudsters. Mr. Bue demands the money subject to the Preservation Order be released to him.

Procedural History

[3] When HoneyBadger became aware that the Credit Union had reversed payments it had received for the purchase of cryptocurrency by Mr. Bue, or rather entities claiming to be Mr. Bue, it commenced this action. Cryptocurrency, once purchased, is irretrievable. It was deposited into an assigned wallet, never to be seen again by the parties to this action. Nonetheless, HoneyBadger was out the cost of the purchase price for the cryptocurrency and sought recovery from Mr. Bue and/or the Credit Union. The Credit Union reversed transactions of $240,000. At the time of drafting the claim, the allegation was that Mr. Bue had received cryptocurrency arising from the purchases and for which he has not paid. HoneyBadger pled breach of contract as Mr. Bue had contracted for cryptocurrency but did not pay for it.

2025 SKKB 123 (CanLII)

[4] Mr. Bue defended the claim on the basis that he did not contract with HoneyBadger to purchase the cryptocurrency but rather the contract to purchase was the work of unknown fraudsters who had taken control of his email and Mr. Bue received no benefit. He further argued the PAD Agreement provided safeguards to prevent unauthorized payments including a requirement that he be given notice to debit his account and a further requirement that there be a password or security code or other signature equivalents to authorize a PAD Agreement payment. He argues he was not warned of the dangers of using the PAD Agreement and was not told $100,000 could be transferred out with only an email request. Mr. Bue admits that purchases made on May 29, 2023 for $10,000 in cryptocurrency and again on May 30, 2023 for $30,000 in cryptocurrency were made by him but the remaining purchases of $200,000 were instigated by the fraudsters.

[5] Mr. Bue pled *The Sale of Goods Act*, RSS 1978, c S-1 asserting there was no written agreement and therefore the contract for the purchase of cryptocurrency was unenforceable. He further alleged HoneyBadger did not comply with the "travel rule" to ensure he owned the bitcoin wallets in question and suggests the agreement is illegal insofar as it does not comply with Financial Transactions and Reports Analysis Centre of Canada [FINTRAC] guidelines.

[6] Mr. Bue counterclaimed against HoneyBadger alleging that as a Money Services Business and FINTRAC registrant, a duty of care was owed to the defendant which included a duty to protect him from fraud and identify the parties to the transactions and a further duty of care arose through operation of the PAD Agreement. Mr. Bue further suggests it was an abuse of process to obtain the Preservation Order thus resulting in further loss to Mr. Bue who could not access his funds.

[7] In response, HoneyBadger asserted it had no knowledge of unknown fraudsters taking control of Mr. Bue's emails. *The Sale of Goods Act* has no application

2025 SKKB 123 (CanLII)

as the cryptocurrency is not a "good" as referenced in the legislation and, in any event, there was a written agreement between the parties. HoneyBadger does not dispute it owed Mr. Bue a duty of care but denies being in breach of that duty as it is not its duty to protect Mr. Bue from fraud perpetrated by unknown and unrelated third parties. HoneyBadger denies non-compliance with the "travel rule" and asserts it obtained the required verifications prescribed by FINTRAC. HoneyBadger further asserts it complied with the terms of the PAD Agreement and denies any wrongdoing in obtaining the Preservation Order.

2025 SKKB 123 (CanLII)

[8] Prior to the close of pleadings, the parties had agreed in July 2023, pursuant to a Consent Order, to freeze the $240,000 at the Credit Union until September 7, 2023. The Order was extended by agreement and ultimately the matter was heard in chambers and a judgment rendered on September 19, 2023 preserving the funds (2023 SKKB 193). The parties now ask that their respective claims be dealt with by way of summary judgment application.

Is this a proper case to be decided on a summary judgment application?

[9] Both HoneyBadger and Mr. Bue agree the matter should be determined by way of summary judgment. Elson J. in *McKercher v Stantec Architecture Ltd.*, 2019 SKQB 100 [*McKercher*], summarized the law in Saskatchewan:

> [24] Most of the jurisprudence of this Court on Rule 7-5 post-dates the Supreme Court of Canada judgment in *Hryniak v Mauldin*, 2014 SCC 7, [2014] 1 SCR 87 [*Hryniak*]. In *Hryniak*, Karakatsanis J. described at length the purpose and key elements of summary judgment applications in Ontario, a description that similarly applies to the interpretation of Rule 7-5. The most frequently cited Saskatchewan decision, which summarized the analysis in *Hryniak*, is the judgment of Barrington-Foote J. (as he then was) in *Tchozewski v Lamontagne*, 2014 SKQB 71, 440 Sask R 34 [*Tchozewski*]. At para. 30 of *Tchozewski*, Barrington-Foote J. described the approach a chambers judge is required to follow. This approach has been endorsed by the Saskatchewan Court of Appeal in three separate decisions, *Deren v SaskPower*

> *and Saskatchewan Watershed Authority*, 2017 SKCA 104; *Haztech Fire and Safety Services Inc. v M. Thompson Holdings Ltd.*, 2017 SKCA 56; and *Viczko v Choquette*, 2016 SKCA 52, [2016] 6 WWR 479.
>
> [25] As the suitability of summary judgment is not significantly disputed in this case, it is not necessary to recite the *Tchozewski* approach verbatim. It is sufficient to reference the more abbreviated description of the approach in *Auchstaetter v Evolution Homes Ltd.*, 2016 SKQB 360 at paras 4 and 5. There, Smith J. observed that the chambers judge must determine whether the issues raised are sufficiently focused and the material is sufficiently detailed to allow the Court to do four things: 1) make the necessary findings of fact; 2) apply the law to those findings; 3) conclude that summary judgment is a proportionate, more expeditious and less expensive means to achieve a just result; and 4) determine whether there appears to be no genuine issue requiring a trial.

[10] HoneyBadger argues this case is suitable for summary judgment as the amount in dispute is relatively modest and the factual record, after cross examination is not controverted. At the heart of the dispute, argues HoneyBadger, is how a PAD Agreement should be interpreted. Mr. Bue, it argues, is in breach of contract and HoneyBadger wants its money. Mr. Bue does not dispute that this is an appropriate case to be determined by way of summary judgment application. However, Mr. Bue argues that if HoneyBadger insists it is Mr. Bue that sent the emails to acquire the cryptocurrency, rather than unknown persons who gained access to his email and made the last two purchases for $100,000 each, then there is a problem.

[11] There is no strong argument advanced by HoneyBadger that Mr. Bue did not send the emails to make the last two purchases of $100,000 each. To suggest as Mr. Bue has, that fraudsters impersonating as the “FBI” gained access to his computer and sent the emails, may be implausible in normal circumstances, but, unfortunately, in Mr. Bue’s case, it is not. HoneyBadger has provided no evidence to suggest Mr. Bue received the benefit of the cryptocurrency other than the purchase requests came from his email.

2025 SKKB 123 (CanLII)

[12] Mr. Bue has been subjected to cross examination and the transcripts have been filed in the proceedings. I accept on the evidence filed that Mr. Bue did not initiate the last two purchases and had no knowledge of the purchases having been made until after the fact. HoneyBadger also argues that further expert evidence should have been filed by Mr. Bue to establish the standard of care required of HoneyBadger considering the allegations of breach of duty of care towards Mr. Bue by violation of the "travel rule" and FINTRAC guidelines. Further evidence on both sides respecting these disputed issues may have been helpful but not fatal to the summary judgment application. As Elson J. described it in *McKercher* at para 26:

> [26] In this consideration, summary judgment applications require each party to put its "best foot forward", irrespective of their belief that a trial is necessary. Accordingly, both parties, particularly those who respond to the application, must confront the reality that this may well be their only "day in court". As I observed at para. 122 of the judgment of this Court in *Deren v SaskPower and Saskatchewan Watershed Authority*, 2015 SKQB 366, aff'd 2017 SKCA 104, a party cannot respond to a summary judgment application simply by saying that the case to be made, either in pursuit of a claim or defence, will present itself in the fullness of time at trial. In making this observation, I relied on the *per curiam* judgment of the Supreme Court of Canada in *Canada (Attorney General) v Lameman*, 2008 SCC 14 at paras 10 and 11, [2008] 1 SCR 372, where the Court said the following:
>
> > [10] This appeal is from an application for summary judgment. The summary judgment rule serves an important purpose in the civil litigation system. It prevents claims or defences that have no chance of success from proceeding to trial. Trying unmeritorious claims imposes a heavy price in terms of time and cost on the parties to the litigation and on the justice system. It is essential to the proper operation of the justice system and beneficial to the parties that claims that have no chance of success be weeded out at an early stage. Conversely, it is essential to justice that claims disclosing real issues that may be successful proceed to trial.

2025 SKKB 123 (CanLII)

> [11] For this reason, the bar on a motion for summary judgment is high. The defendant who seeks summary dismissal bears the evidentiary burden of showing that there is "no genuine issue of material fact requiring trial": *Guarantee Co. of North America v. Gordon Capital Corp*., [1999] 3 S.C.R. 423, at para. 27. The defendant must prove this; it cannot rely on mere allegations or the pleadings: *1061590 Ontario Ltd. v. Ontario Jockey Club* (1995), 21 O.R. (3d) 547 (C.A.); *Tucson Properties Ltd. v. Sentry Resources Ltd.* (1982), 22 Alta. L.R. (2d) 44 (Q.B. (Master)), at pp. 46-47. If the defendant does prove this, the plaintiff must either refute or counter the defendant's evidence, or risk summary dismissal: *Murphy Oil Co. v. Predator Corp.* (2004), 365 A.R. 326, 2004 ABQB 688 at p. 331, aff'd (2006), 55 Alta. L.R. (4th) 1, 2006 ABCA 69. Each side must "put its best foot forward" with respect to the existence or non-existence of material issues to be tried: *Transamerica Life Insurance Co. of Canada v. Canada Life Assurance Co.* (1996), 28 O.R. (3d) 423 (Gen. Div.), at p. 434; *Goudie v. Ottawa (City)*, [2003] 1 S.C.R. 141, 2003 SCC 14 at para. 32. The chambers judge may make inferences of fact based on the undisputed facts before the court, as long as the inferences are strongly supported by the facts: *Guarantee Co. of North America*, at para. 30.
>
> [Emphasis added in original]

[13] I agree with counsel that this is an appropriate case to be determined by summary judgment. Findings of fact can be made, and the law can be applied to those findings. Although better evidence may have been produced on some issues, the parties have a responsibility to put their best foot forward on a summary judgment application. It is a proportionate and expeditious means to achieve a just result and there appears to be no genuine issue requiring a trial.

2025 SKKB 123 (CanLII)

Analysis

History

[14] Mr. Bue's financial tale of woe is outlined in correspondence he sent to one of his scammers and exhibited as Exhibit A to his Affidavit sworn May 14, 2024 and begins long before he made contact with HoneyBadger. It began in 2022 when he "invested" with an entity which went by the name Main Bit Ltd. Unfortunately for Mr. Bue, he had clicked on an item of interest while surfing the net and was lured into a virtual den of thieves. The business turned out to be a scam and Mr. Bue, after numerous transactions to buy cryptocurrency in the amount of $53,873, lost all contact with Main Bit Ltd. when he tried to cash in his investment.

[15] Mr. Bue was then contacted on September 22, 2022 by the "Ministry of Justice at the United Kingdom" and was informed that the "Ministry" could help him provided he sent some money to begin the process. He was told that because his initial investment with Main Bit Ltd. was put into cryptocurrency, the investment would have increased due to market forces, and he would be entitled to more money than had been originally invested.

[16] Mr. Bue transferred $19,600 initially and then over the course of several weeks sent $170,906.61 in Canadian funds. Ultimately in or around December of that year, he was contacted and informed another $75,000 USD was needed and, at this point, Mr. Bue allegedly told them in no uncertain and colourful terms that he had nothing more to give. Nonetheless, he claims in the correspondence that at the "Ministry's" request, he obtained a letter from his financial institution saying this could not be financed by his financial institution. There is no explanation as to why Mr. Bue's financial institution did not step in to the fray to protect him insofar as the financial institution appears to have had notice of his dealings but the financial institution in question is no longer part of these proceedings. Contact with the "Ministry" came to an

2025 SKKB 123 (CanLII)

end when no further funds were available.

[17] On January 25, 2023 Mr. Bue was contacted via email by "Funds Recall". The entity identified itself as a "Cybercrime agency" that had come across his "details in data files captured from servers of one of the groups" being investigated. Main Bit Ltd. was referenced in the email. Despite receiving this correspondence, Mr. Bue does not appear to have given cash to "Funds Recall".

[18] However, he was soon duped again when he was contacted by email from an individual purporting to be with the "FBI". The "FBI" contacted him via a gmail address and explained to Mr. Bue that he had fallen victim to a scam by these former entities. The "FBI" requested Mr. Bue's participation in a "dummy money transfer" to assist in dismantling the illegal operation. It was after being contacted by the "FBI" that Mr. Bue reached out to HoneyBadger to purchase cryptocurrency. The "FBI" provided Mr. Bue with a bitcoin wallet which he forwarded to HoneyBadger.

[19] Two purchases were made, one by wire transfer on April 27, 2023 and another by account debit on May 1, 2023, collectively for $79,991.07. Mr. Bue also gave the "FBI" remote access to his computer via an app called "AnyDesk". He had to give permission each time they gained access but claims to have watched what they were doing only 90-95% of the time. Mr. Bue may have also provided access to his email accounts but whether it was access through email passwords or simply access through his computer is unknown.

[20] Mr. Bue made two more purchases, one on May 29, 2023 for $10,000 and one on May 30, 2023 for $30,000. However, two more purchases were made, one on May 31st and one on June 1st for a total of $200,000 which Mr. Bue knew nothing about until he saw the state of his account. Given that he had provided the "FBI" with access to his computer, he suspects the "FBI" made the purchases. Mr. Bue does not have possession of the bitcoin wallet and is out hundreds of thousands of dollars since his

2025 SKKB 123 (CanLII)

initial contact with Main Bit Ltd. in 2022. Mr. Bue then contacted his financial institution, the Credit Union who, pursuant to the PAD Agreement, seized $240,000 which amount was then made the subject of the Preservation Order.

2025 SKKB 123 (CanLII)

The PAD Agreement

[21] At no time did Mr. Bue inform anyone he spoke to at HoneyBadger of his experiences with the various ne'er-do-wells with whom he had been doing business, nor did he relate that he was working with the "FBI". Mr. Bue's first transaction with HoneyBadger was done by wire transfer. He reached out to HoneyBadger customer support on April 25, 2023 indicating he wanted to purchase $48,000 in bitcoin. Mr. Esselmont, an employee at Honeybadger, reached out to Mr. Bue via email to confirm the purchase request and explained how to make the wire transfer. He further advised that once the transfer was received, he would send a quote emailing the bitcoin pricing and upon receiving an email from Mr. Bue confirming acceptance of the price, the bitcoin would be deposited to his wallet.

[22] On April 27, 2023, Mr. Esselmont suggested to Mr. Bue that HoneyBadger could also set up a PAD (pre-authorized debit) with Mr. Bue which could prove more convenient as Mr. Bue would no longer have to attend at his financial institution to complete a wire transfer. Further information was sent to Mr. Bue on April 28, 2023 respecting the PAD and how it operates. By email, Mr. Esselmont provided the PAD form and explained how to complete the form. He then went on to explain:

> The rest of the purchase process is as follows:
>
> 1. Once I receive the items above, I'll initiate the PAD on your account. It typically takes -4 hours for funds to be credited to our account.
>
> 2. Once funds are received, we will lock in BTC/CAD pricing. I'll send you a quote by email indicating the amount of BTC purchased less our 6% fee.

> 3. You reply by email “CONFIRMED” and I’ll send your BTC to your wallet address.
>
> 4. BTC arrives in -10 min. I’ll send your receipt link to view your transaction on the blockchain.”
>
> [Affidavit of Shea Esselmont sworn March 13, 2024, Exhibit E]

[23] Mr. Bue responded within three minutes to advise, “I accept the terms”. Mr. Bue then completed the PAD Agreement and made several purchases with HoneyBadger removing funds from his account. On May 1, 2023 he purchased $32,000. On May 29, 2023 he purchased $10,000 and on May 30, 2023 he purchased $30,000. Mr. Bue admits to having made those purchases and does not take the position they were unauthorized though he did not receive the money as it was deposited to the wallet given to him by the “FBI”. On May 31 and on June 1, 2023 two more purchases of $100,000 were made via withdrawal of funds from his account and Mr. Bue claims these latter two purchases were unauthorized and made without his knowledge or consent.

[24] The PAD Agreement was a signed contract between Mr. Bue and HoneyBadger. The form appears to have been partially completed by HoneyBadger as it is partially typed with the missing information completed in handwriting by Mr. Bue. Mr. Bue completed his name and mailing address but left both his phone and email blank. He listed his financial institution as Innovation Credit Union in Cabri, Saskatchewan and provided the bank account number. HoneyBadger had marked the agreement as variable. Although there was a line to note the maximum amount of withdrawal, this was not completed. The PAD Agreement also indicated the withdrawals were to be sporadic. Mr. Bue signed and dated the agreement April 28, 2023. The terms and conditions of the agreement are on page 2 of the agreement. The agreement provided at para. 8:

2025 SKKB 123 (CanLII)

> 8. If this agreement provides for PADS with sporadic frequency, I/we understand that the Payee is required to obtain an authorization from me/us for each and every PAD prior to the PAD being exchanged and cleared. I/we agree that a password or security code or other signature equivalent will be issued and will constitute valid authorization for the Processing Institution to debit the Account.
>
> [Affidavit of Shea Esselmont sworn March 13, 2024, Exhibit C]

[25] HoneyBadger maintains that "Mr. Bue authorized all debits to his account via email, using email accounts that he had expressly authorized HoneyBadger to use. Mr. Bue agreed to use email authorization as the means (signature equivalent which Clause 8 provides for) by which his account could be debited, including as evidenced by the fact that he did not dispute several purchases made via PAD with HoneyBadger, all of which were confirmed via email." (Brief of law on behalf of HoneyBadger, para. 46)

[26] There is no dispute that Mr. Bue agreed to the terms suggested by Mr. Esselmont which allowed for an approval of the purchase of bitcoin by emailing "confirmed". The argument presented by Mr. Bue is that clause 8 of the PAD Agreement requires that "a password or security code or other signature equivalent will be **issued (**emphasis added) and will constitute valid authorization for the Processing Institution to debit the Account".

[27] Although an email may, in certain circumstances, operate as a signature equivalent, it is difficult to reconcile an email from Mr. Bue's address as being a signature equivalent when the "password, security code or signature equivalent" must be issued by HoneyBadger. What is being described in the PAD Agreement would suggest a further step in the verification process to begin the withdrawal. Nothing in Mr. Esselmont's email explains how to commence a PAD withdrawal. Mr. Esselmont's email speaks of confirming a purchase once a debit is made via email but does not address how Mr. Bue is to initiate a purchase request.

2025 SKKB 123 (CanLII)

[28] Mr. Bue had been sending email requests to make purchases. Accepting the same email(s) without any means of verifying that it is in fact the person claiming to be Mr. Bue would appear to be in contravention of the express wording of the PAD Agreement. HoneyBadger did not "issue" anything to Mr. Bue. Complacency or failure to object on Mr. Bue's part, does not change the requirements of the terms of the PAD. The fact that Mr. Bue went along with email purchase requests without verification for the first few purchases does not alter the fact that was not what the PAD Agreement required. In essence, the process HoneyBadger followed worked until it did not. Why the Credit Union went along with this process and debited the account in spite of the clear wording of the PAD Agreement is an unknown. However, the Credit Union is no longer a party to these proceedings.

The Sale of Goods Act

[29] Mr. Bue has defended on the basis that *The Sale of Goods Act* applies but as HoneyBadger has argued, cryptocurrency is not a "good" and the agreements are in writing. *The Sale of Goods Act* describes a "good" as follows: "goods" includes all chattels personal other than things in action or money and includes emblements, industrial growing crops and things attached to or forming part of the land which are agreed to be severed before sale or under the contract of sale". Clearly cryptocurrency did not exist at the time the legislation was drafted.

[30] In *Copytrack Pte Ltd. v Wall*, 2018 BCSC 1709, the Court refused to characterize cryptocurrency commenting:

> [34] In my view, the proper characterization of cryptocurrency, including the Ether Tokens, is a central issue in this case, and one that informs the analysis of whether Copytrack's claims in conversion and detinue can succeed. However, the evidentiary record is inadequate to permit a determination of that issue on this application, and, in any event, it is a complex and as of yet undecided question that is not suitable for determination by way of a summary judgment

2025 SKKB 123 (CanLII)

application.

[31] In *Ramirez v Ledn Inc.*, 2023 ONSC 3716, the Court refused to consider the tort of conversion as "Bitcoins are intangible property" (para. 110).

[32] Regardless of whether cryptocurrency is a "good" or not, there is memorandum in writing respecting the transactions and therefore Mr. Bue's statutory defence must fail.

Was there a valid contract for the purchase and sale of bitcoin between HoneyBadger and Mr. Bue for the two $100,000 transactions?

[33] The agreement to purchase the cryptocurrency between Mr. Bue and HoneyBadger was reduced to writing in the form of an email exchange which HoneyBadger refers to as the Transaction Agreement and Mr. Bue confirmed the terms. However each transaction was a separate agreement. Mr. Bue asked to purchase cryptocurrency, HoneyBadger withdrew the funds pursuant to the Pad Agreement, and advised of pricing. Mr. Bue then accepted the price and the cryptocurrency was deposited to his wallet. This proceeded without incident for the first couple of transactions. However, for the latter two purchases, it was not Mr. Bue who was the party to the contract but rather unknown parties impersonating Mr. Bue.

[34] In fairness to HoneyBadger, the request to buy the $100,000 bitcoin on May 31, 2023 and June 1, 2023 came from Mr. Bue's email account, in the same manner that it had before. The difference, however, is that for these latter two purchases, it was not Mr. Bue sending the emails from the email account. His computer had been taken over by the "FBI". HoneyBadger asserts that it followed the procedure for purchases as had been agreed to in the letter of April 27, 2023 and when Mr. Bue directed the Credit Union to reverse the transactions, he was in breach of contract and HoneyBadger is entitled to the funds.

2025 SKKB 123 (CanLII)

[35] Mr. Bue, on the other hand, argues it is not his contract and cannot be responsible for the purchases. Mr. Bue relies on *Saint John Tug Boat Co. Ltd. v Irving Refining Ltd.*, [1964] SCR 614, in support of his contention that both parties must objectively manifest their intention to be bound by the agreement. As Mr. Bue had no knowledge of the transactions when they occurred, the transactions were initiated by unauthorized third parties and Mr. Bue received no benefit, there could be no contract formation.

[36] HoneyBadger argues it followed the procedure which Mr. Bue had confirmed with Mr. Esselmont and argues the facts are not dissimilar to those found in *Du v Jameson Bank*, 2017 ONSC 2422. Mr. Du had opened an account with Jameson Bank and communicated with the bank by email to effect transfers. A third party gained access to his email and funds were wired to Singapore which resulted in Mr. Du bringing an action against the bank. The Court made the following comments respecting breach of contract:

> **The Breach of Contract**
>
> [55] At the time of the critical events in issue; namely May 2012, Jameson had a contractual relationship with Du which can be best described as a creditor and debtor relationship. Jameson was not in any type of advisory relationship with Du. Du opened a foreign exchange account with Jameson which specifically permitted him to give instructions electronically to Jameson through a specific email address controlled solely by Du.
>
> [56] Jameson had a common law and contractual obligation to honour its customers' instructions and was entitled to treat its customer's mandate at its face value. Jameson was required to act on its customers instructions so long as he or she had sufficient credit. Pursuant to the terms of the agreement, Jameson was not obligated to question any transaction which was in accordance with its mandate and was not required to question the instructions received for Du's account.
>
> [57] In this case, Jameson was merely complying with the instructions received from Du via the email address provided by

2025 SKKB 123 (CanLII)

him in his application. This is the same email address subsequently used for the purposes of communicating instructions for an authorized transfer on February 6, 2012. Jameson had no reason to believe the instructions to wire transfer money from Du's foreign exchange account to beneficiaries located in Singapore, received just over two months later, were fraudulent. The emails made reference to Du's personal banker "Julie" at BNS and to a cheque that had been delivered to BNS for certification and disclosed other details that could only be known to Du.

[58] Moreover, Jameson was acting in accordance with the contract that governed the relations between it and Du. Du executed a contract acknowledging that he received the terms and conditions of the account agreement. The law is clear that a person is bound by an agreement to which they put their signature whether they have read the agreement's contents or have chosen to leave then unread. Our Court of Appeal has held in *Fraser Jewellers (1982) Ltd. v. Dominion Electric Protection Co.* (1997), 34 O.R. (3d) 1 (Ont. C.A.) that failure to read a contract before signing it is not a legally acceptable basis for refusing to abide by it:

> As a general proposition, in the absence of fraud or misrepresentation, a person is bound by an agreement to which he has put his signature whether he has read its contents or has chosen to leave them unread: Cheshire, Fifoot & Furmston's Law of Contract, 13th ed. (1996) at p. 168. Failure to read a contract before signing it is not a legally acceptable basis for refusing to abide by it. A businessman executing an agreement on behalf of a company must be presumed to be aware of its terms and to have intended that the company would be bound by them. The fact that Mr. Gordon chose not to read the contract can place him in no better position than a person who has. Nor is the fact that the clause is in a standard pre- printed form and was not a subject of negotiations sufficient in itself to vitiate the clause: *L'Estrange v. F. Graucob Ltd.*, [1934] 2 K.B. 394 at p. 403, [1934] All E.R. Rep. 16 (D.C.); *Craven v. Strand Holidays (Canada) Ltd*. (1982), 40 O.R. (2d) 186 at p. 194, 142 D.L.R. (3d) 31 (C.A.).

[59] In this case, Du admitted that he does not read agreements with banks as a matter of practice. In his affidavit filed in response, he attempted to argue that the signed

2025 SKKB 123 (CanLII)

application was not a contract but conceded in cross-examination, however, that he did not see the difference between the contract and an application form.

[60] In the absence of fraud or misrepresentation, the signature of a party who signs a contract is irrefutable evidence of the signers' assent to the whole contract. There is no evidence that Jameson made any misrepresentation or acted fraudulently in connection with the opening of Du's foreign exchange account or the execution of the application and account agreement.

[61] When a customer executes an agreement and confirms having received the terms and conditions, our courts have determined that customers are bound by those terms. Du executed the contract acknowledging that he received a copy of the account terms and conditions at that time. By those terms, Du was made aware of the risks associated with providing instructions via email and knew that he was obligated to protect the integrity of his email account.

[62] The terms of the application and the account agreement are clear. Du was entitled to provide instructions to Jameson by email address and he did so without complaint to effect a wire transfer to a US account shortly after his opening of the foreign exchange account. Jameson was contractually entitled to rely on those instructions. Du had the sole ability and responsibility to control the security of the email account which was the source of the impugned transactions.

[63] There was no obligation in law for Jameson to question the purported transfer. Jameson's compliance with the instructions received from Du's email address did not breach any internal policy or any term of the agreement. The money value of the wire transfers did not require Jameson to obtain his further authorization and confirmation.

[64] In addition, there is no liability because of the contractual exclusion contained in the agreement. Du has failed to establish that Jameson was "grossly negligent" or that it acted with "wilful misconduct." Jameson complied with the instructions received from Du's email address; an email address he included in the application and which he had used to communicate with Jameson from the time his account was opened. The questioned email communications contained information with respect to Du's personal banker and the delivery of a certified cheque, and as such, Jameson had no reason to doubt the authenticity of the

2025 SKKB 123 (CanLII)

> email communications. The fact that a customer is a victim of fraud does not result in an automatic transfer of liability to the customer's bank.
>
> [Footnotes omitted]

[37] HoneyBadger suggests that as the same circumstances arose with Mr. Bue, a similar result should follow. There are, however, some differences. Although Mr. Du claims not to have read the contract with the bank, the terms of the contract clearly set out his responsibilities and the bank's limited liability. The Jameson Bank specified that there were risks associated with using electronic communications but nonetheless Jameson Bank could rely on such communications. The relevant provisions are as follows, at para. 9:

> 2.2 Reliance on Instructions. Jameson may rely and act upon telephone, facsimile transmission and any other electronically transmitted instructions from or purporting to be from you (including an authorized person) and which Jameson believes in good faith to be genuine.
>
> 5. Wire transfers
>
> d) Absent gross negligence or wilful misconduct by Jameson or any of its employees, Jameson shall not be responsible or liable for any damages, losses, expenses or the like that you may directly or indirectly incur or arising from or in connection with any wire transfer. Jameson shall not be responsible for any failure, unavailability or malfunction of communications, electronic or other equipment which may result in misdelivery, nondelivery or delays in delivery of the funds transferred nor shall it be held responsible for the insolvency, neglect, conduct, mistake, default, delay, misappropriation, negligence or breach of contract by any other bank, entity or person, in connection with the wire transfer, without regard to any agency relationship those persons or entities may have with Jameson.
>
> 7. Limitation of Liability
>
> 7.3 Your Responsibility. (A) You are responsible to ensure the accuracy of settlement and delivery instructions in respect of each and every Deal (including, but not limited to, any wire instructions). Jameson shall not, in the absence of gross

2025 SKKB 123 (CanLII)

> negligence or wilful misconduct on the part or that of its employees, be responsible for failure, delays or errors in the receipt of such instructions and Jameson shall have no liability for consequential or special damages. (B) You agree to maintain security systems, procedures and controls to prevent and detect (i) the theft of funds; ii) forged, fraudulent and unauthorized instructions and electronic transfer of funds by anyone who is not an Authorized Person; (iii) losses due to fraud or unauthorized access to the service by anyone who is not an Authorized Person.
>
> . . . .
>
> (D) . . . You agree to keep any keys, access codes, security devices and verification procedures safe and confidential, and change them at least as often as the service materials specify. We may establish a routine to verify the source and authenticity of instructions you give us and may verify an instruction before acting on it. We may act on instructions that contain the verification routine without checking the authority.
>
> 8.6 Electronic Communications. Jameson may maintain a database in respect of all of your instructions, including recordings of telephone conversations. Jameson's records will be conclusive and binding on you in any dispute, including in any legal proceeding, as the best evidence of your Deals, in the absence of clear proof that Jameson's records are erroneous or incomplete. . . . You agree with Jameson that notwithstanding the risks associated with electronic communications, you hereby authorize Jameson to provide such services in compliance with the procedures established by Jameson from time to time. Any electronic communication that Jameson receives from you or in your name will be considered to be duly authorized and binding upon you. Jameson will be authorized to rely and act upon any signature appearing on a facsimile transmission that purports to be the signature of an Authorized Person.

[38] No such provisions formed any part of the agreement between HoneyBadger and Mr. Bue. The use of email was a practice that had developed between HoneyBadger and Mr. Bue but Mr. Bue's email address is not mentioned in the PAD Agreement and the PAD Agreement itself makes reference to the requirement to "issue" a password, security code or signature equivalent. It follows that although the facts in the above case are similar insofar as a third party used the email of another to obtain

2025 SKKB 123 (CanLII)

funds, that is where the similarity ends. Mr. Bue's money was sent to HoneyBadger in error and not at his request.

[39] In *Bank of Montreal v Asia Pacific International Inc.*, 2018 ONSC 4215 [*Asia Pacific*], a similar situation was addressed where the Bank of Montreal [BMO] sent monies via wire transfer at the request of a client but later learned the person who instigated the wire transfer was not a client but rather an imposter. Asia Pacific International Inc. [API] received the wire transfer at its Toronto-Dominion [TD] account and completed a sale of gold. The TD bank did not release the funds to API upon being notified by the BMO of the fraud. API was out the gold and wanted the funds as a result.

[40] BMO had repaid its client the money which had been wired as she had never been authorized the wire. BMO then argued it had forwarded the funds to API under a mistake of fact. API should have known the purchase was fraudulent as there were grounds to be suspicious and it cannot rely on the defence of change of position because it was in breach of its obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 and *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulation*, SOR/2002-184 by failing to obtain information and report suspicious circumstances.

[41] API, on the other hand, argued BMO was in a better position to prevent the fraud and failed to exercise due diligence. The Court considered *Rogers v Priyance Hospitality Inc.*, 2016 ONSC 7851 where the Court had to consider who should bear the loss out of two innocent victims of fraud. Mr. Rogers had relied on *Marvco Colour Research Ltd. v Harris*, [1982] 2 SCR 774 which Nishikawa J. summarized in *Asia Pacific* as standing for the following principles:

> [38] …1) that as between two innocent parties, justice requires that the party who was in a position to prevent the loss should bear it; and (ii) a person who takes money obtained by

2025 SKKB 123 (CanLII)

> fraud, but takes it in satisfaction of a *bona fide* debt, is entitled to retain it.

[42] Ultimately, although it was found API could have shown more diligence, BMO, through its "careless conduct" exposed API to the risk of loss and API was entitled to retain the funds. Nishikawa J. also considered BMO's argument of the payment having been made by mistake of fact but found BMO was capable of discovering the imposter before completing the wire transfer and, in any event, if there was payment made by mistake of fact, API had changed its position. His findings are summarized at paras. 53 and 54:

> [53] In my view, in the event that BMO paid the funds under a mistake of fact, API would be entitled to rely upon the doctrine of change of position. Once API knew that the wired funds were in its account, and verified the original wire transfer documents, API released the gold bars to Filali. API thus changed its position in reliance on the wire transfer having been duly authorized. Had API known that the wire transfer was fraudulent, it would not have released the gold. API is in the position of having released the gold without having received payment for them.
>
> [54] The question that remains is whether API's change of position was in good faith, or whether API engaged in wrongful conduct that would preclude its recovery of the funds. The change of position defence is not be (*sic*) available to a wrongdoer, as determined by the Supreme Court in *Garland v. Consumers' Gas Co.*, 2004 SCC 25, [2004] 1 S.C.R. 629…

[43] The Court concluded at para. 74:

> [74] … There is insufficient evidence of wrongdoing on API's part, such that it would not be entitled to rely upon the defence.
>
> [75] The fact remains that had the fraudulent wire transfer not been authorized by BMO, API would not have found itself the target of Filali's fraudulent purchase. In *Clark v. Eckroyd* (1886) 12 O.A.R. 425, the Court of Appeal for Ontario found that the payor was entitled to recover because the careless conduct of the recipient in releasing goods that had not been paid for commend

2025 SKKB 123 (CanLII)

> the chain of events leading to the loss. Similarly, in this case, it was the careless conduct of BMO that initiated the chain of events leading to the loss.

[44] There can be no doubt in these circumstances that Mr. Bue's naivete and ignorance is at the heart of this fraud. He was duped several times but nonetheless cooperated fully with fraudsters purporting to be the "FBI". Mr. Bue not only made purchases and deposited those purchases to a wallet willingly, he opened his computer and allowed the "FBI" free access. Had Mr. Bue made mention of any of what was transpiring to HoneyBadger, the fraudulent scheme would have come to an abrupt end. Unfortunately, he kept his silence and thereby permitted the fraudsters to acquire $200,000 in cryptocurrency over and above the amounts he had already purchased on their behalf.

[45] There is nothing in the transactions between Mr. Bue and HoneyBadger which would have raised alarms. Mr. Bue's conversations on the phone and his emails with HoneyBadger raise no alarms. The fact that the amount of the cryptocurrency being purchased increased over time was, as HoneyBadger explains, normal practice as people will quite often begin with small purchases which will increase in size once they have a greater level of comfort. But for Mr. Bue's carelessness in allowing the "FBI" access to his computer which they utilized to request purchases, HoneyBadger would not have drawn on the PAD or released the cryptocurrency. HoneyBadger, at all times, believed it was dealing with Mr. Bue. However, has there been wrongdoing on the part of HoneyBadger which would disentitle it from a full recovery of the funds?

FINTRAC

[46] Mr. Bue has argued that HoneyBadger has failed to comply with its obligations as prescribed by FINTRAC and, as such could have prevented the loss. A similar argument was made in *CIBC v Bloomforex Corp.*, 2020 ONSC 69 though Penny J. refused to address the matter in a summary judgment proceeding. Bloomforex

2025 SKKB 123 (CanLII)

received funds for the purchase of Chinese yuan. The Canadian Imperial Bank of Commerce and the Bank of Montreal clients were the victims of the fraud and the banks, having made the clients' whole, sought recovery from Bloomforex. Bloomforex changed its position having received the funds and converted it to yuan. The Court commented at para. 21, "It must be noted that there is nothing *per se* illegal about the transactions effected by Bloomforex (assuming no knowledge of the initiating fraudulent transfers). However, Canada's anti-money laundering legislation does apply to money services businesses like Bloomforex…"

2025 SKKB 123 (CanLII)

[47] The parties had filed expert evidence respecting Bloomforex's obligations at law. The Court ultimately concluded that a trial would be required commenting at para. 31:

> [31] Parties on a motion for summary judgment are generally required to put their "best foot forward". However, the nature and complexity of the issues sometimes demand that the normal process of production and oral discovery be completed before a party can be called upon to put their "best foot forward," *Combined Air Mechanical Services Inc. v. Flesch*, 2011 ONCA 764 at para 57.

Penny J. declined to grant summary judgment.

[48] Like Penny J., I am unable on the evidence filed to conclude whether HoneyBadger has complied with its obligations pursuant to FINTRAC. HoneyBadger suggests there has been compliance, Mr. Bue claims there has not. HoneyBadger argues Mr. Bue should have tendered expert evidence as to its requirements if it wished to argue non-compliance with FINTRAC. However, HoneyBadger could also have filed such expert evidence to confirm its compliance. The issue of whether there has been non-compliance with the "travel rule" as prescribed by FINTRAC is a question which would have to proceed to trial, but unlike *Bloomforex* where the parties filed expert evidence and cross examination was required, no evidence was led as to what might be expected for there to be proper compliance with the "travel rule". There is no indication

such evidence would be called if the matter proceeded to trial. The parties are to put their best foot forward and, on this issue, they have not. In the circumstances, given the lack of evidence on this issue, I cannot conclude HoneyBadger has failed to comply with its FINTRAC obligations.

Of the two innocent victims, who should receive the funds?

[49] Notwithstanding that I am unable to make a determination on the "travel rule", there is evidence of wrongdoing insofar as there has been non-compliance with the PAD Agreement. HoneyBadger was required to "issue" a password or signature equivalent but chose instead to rely on email communications only.

[50] Clearly Mr. Bue is blameworthy in allowing unknown third parties describing themselves as the "FBI" access to his computer. It was this carelessness that allowed the loss to occur in the first place. However, had HoneyBadger abided by the terms of the PAD Agreement and "issued a password or signature equivalent", the fraud would have been stopped before HoneyBadger parted with the cryptocurrency.

[51] In *Isaacs v Royal Bank of Canada*, 2011 ONCA 88, the Ontario Court of Appeal upheld the decision of the Court below which found in favour of the bank where two innocent victims of fraud were duped by fraudsters. The bank's conduct, at its highest, was careless. But the appellant's conduct was more than careless. It involved affirmative action on her part that facilitated the **fraud**. This is a significant distinction between the nature of the parties' conduct:

> [7] This factor also distinguishes this case on the facts from *Marvco Color Research Ltd. v. Harris*, [1982] 2 S.C.R. 774 (S.C.C.), where **two innocent** parties fell **victim** to **fraud** by third parties. In this case, as we have said, both parties were careless. However, both parties were not **innocent** of any wrongdoing. On these facts, where the carelessness of one party involves active participation in the fraudulent scheme and results in the wrongdoing being able to inflict the loss, that party must

2025 SKKB 123 (CanLII)

> bear the burden of the loss.
>
> [Emphasis added]

[52] There is no doubt that with respect to the purchases initiated by Mr. Bue on behalf of the "FBI" and deposited to their wallet as part of the "dummy transactions" to uncover the frauds perpetuated against Mr. Bue by the previous fraudsters, he was an active participant and is not entitled to recuperate any of his funds. The line is less clear with respect to the $200,000 purchases of which he was unaware.

[53] In *Alfagomma Inc. v HSBC Bank Canada*, 2022 QCCS 3655 [*Alfagomma Inc.*], the Quebec Superior Court was called upon to consider who should bear the loss as between Alfagomma Inc. [Alfagomma] and HSBC Bank Canada [HSBC] where Alfagomma had fallen victim to a fraud of roughly two million dollars and it was alleged HSBC was negligent in accepting the transactions. Ultimately, the Court found that HSBC's actions had fallen short of expected practices. HSBC then argued it was not wholly responsible for the harm claiming Alfagomma's conduct fell below that of a prudent business operation and the company committed faults that caused the loss. The Court acknowledged this was a factor:

> [146] First, the bank argues that in falling for the fraud, Mr. Blanco and Mr. Sacchetti were "credulous" - i.e., they were unreasonably naïve or gullible. Second, Alfagomma's internal controls were deficient, leaving them vulnerable to attack.
>
> [147] HSBC is correct that its liability for the faults it committed may be limited if it establishes that one or other of these alleged Alfagomma faults is also the logical, direct, and immediate cause of its loss. In such a case, the Court must apportion liability based on an assessment of the relative gravity of each fault.
>
> [148] As Professor Vincent Karim explains, the determination of a direct cause of harm does not exclude a finding of contributory negligence:
>
> > La recherche de la cause directe ou du lien de causalité

2025 SKKB 123 (CanLII)

> n'a pas pour effet d'empêcher de retenir plus d'une faute pour expliquer la réalisation du préjudice. Ainsi, un préjudice peut être dû aux fautes combinées du défendeur, de la victime ou d'un tiers. Il est donc possible alors de réduire la responsabilité du défendeur, en fonction de la gravité de sa propre faute, en opérant un partage de la responsabilité. Ce partage s'effectue selon la gravité respective des fautes de chacun des participants au préjudice. Il va de soi que ce genre de partage est, dans la plupart des cas, le résultat d'une évaluation arbitraire car la gravité d'une faute ne peut se mesurer que de façon approximative.
>
> [Footnotes omitted]

2025 SKKB 123 (CanLII)

[54] After a thorough assessment of both parties' conduct, the Court found them equally liable for the loss and apportioned it accordingly. Alfagomma had argued HSBC was in a better position then for it to identify the fraud but the Court ruled at para. 172:

> [172] First, Alfgomma's negligence is not to be underestimated. A person cannot leave their door unlocked and blame a robbery entirely on the police negligently patrolling the neighbourhood.

[55] Similarly, Mr. Bue not only left the door unlocked, he welcomed the robbers in the door and gave them full access for thievery. Allowing the fraudsters full access to his computer and having told no one of his plight despite having already been the victim of previous frauds defies belief but for the fact that he has clearly been defrauded several times over. Had HoneyBadger issued a password or otherwise complied with para. 9 of the PAD Agreement, it may have discerned and prevented the fraud. Like, *Alfagomma Inc*., however, "This is not a case of *novus actus interveniens* but rather of shared responsibility for the harm suffered." (para. 166) On first glance, Mr. Bue who was both naïve and careless should own what he did but in considering that had HoneyBadger complied with the terms of the PAD Agreement, the $200,000 loss may have been prevented. It follows that both must share the responsibility

accordingly. Of the $240,000 being held, $140,000 should be returned to HoneyBadger and the remaining $100,000 to Mr. Bue. The initial $40,000 purchase of cryptocurrency was requested by Mr. Bue. Compliance with the PAD Agreement would have made no difference as Mr. Bue wished to buy cryptocurrency. Had he been issued a password or some other means of verification, he would have complied as he wished to make the purchase. The $40,000 must therefore be repaid to HoneyBadger. Of the remaining $200,000 both Mr. Bue and HoneyBadger share equally in the resulting loss; Mr. Bue for allowing the thieves access and HoneyBadger for failing to utilize a verification process as outlined in the PAD Agreement.

Abuse of Process

[56] Mr. Bue had further argued an abuse of process on the part of HoneyBadger in securing the funds. The Preservation Order was not appealed. HoneyBadger was entitled to avail itself of its remedies at law. There is no justification for such a claim.

Conclusion

[57] HoneyBadger is entitled to $140,000 of the monies subject to the Preservation Order and Mr. Bue is entitled to $100,000. Both parties have achieved a measure of success in these proceedings and, as such there shall be no order as to costs.

J.
C.M. RICHMOND

2025 SKKB 123 (CanLII)