Court of Appeal for Saskatchewan
Docket: CACV4635

Citation: *HoneyBadger Enterprises Ltd. v Bue*, 2026 SKCA 40
Date: 2026-03-13

Between:

HoneyBadger Enterprises Ltd.

Appellant/Respondent by Cross-appeal (Plaintiff)

And

Norman Bue

Respondent/Appellant by Cross-appeal (Defendant)

Before:	Caldwell, Kalmakoff and Bardai JJ.A.
Disposition:	Appeal allowed; cross-appeal dismissed
Written reasons by:	The Honourable Justice Neal W. Caldwell
In concurrence:	The Honourable Justice Jeffery D. Kalmakoff The Honourable Justice Naheed Bardai
On appeal from:	2025 SKKB 123, Swift Current
Appeal heard:	January 23, 2026
Counsel:	Jared D. Epp for the Appellant Jean P. Jordaan for the Respondent

Caldwell J.A.

I. OVERVIEW

[1] HoneyBadger Enterprises Ltd. brokers the purchase and sale of cryptocurrency. Someone posing as the "FBI" used Norman Bue's business relationship with HoneyBadger to fraudulently make off with $240,000 in Bitcoin cryptocurrency. HoneyBadger sued Mr. Bue to recover the funds used to purchase the Bitcoin. In a summary judgment, a judge of the Court of King's Bench ruled that Mr. Bue and HoneyBadger were equally liable for the loss resulting from the fraud and awarded the recovered purchase funds accordingly (*HoneyBadger Enterprises Ltd. v Norman Bue and Innovation Credit Union*, 2025 SKKB 123 [*Judgment*]). HoneyBadger appeals and Mr. Bue cross-appeals from that result, each claiming entitlement to more of the funds.

[2] The fraudulent Bitcoin transactions occurred after Mr. Bue provided a third party with passwords that allowed online access to his computer and to the email account he used when purchasing Bitcoin from HoneyBadger. The identity of the third party is unknown. Using its unsupervised access to Mr. Bue's computer and his accounts, the third party arranged for Mr. Bue to purchase $240,000 in Bitcoin through HoneyBadger over four days, which was deposited into the third party's cryptocurrency wallet.

[3] Five days after the last deposit, Mr. Bue notified HoneyBadger that he had not authorised the Bitcoin purchases. Pursuant to a pre-authorised debit [PAD] agreement with Mr. Bue and his credit union, HoneyBadger had debited the purchase funds from Mr. Bue's account with the credit union. When he objected to the transactions, Mr. Bue's credit union reversed the purchase-price debits. The litigation over who is entitled to those funds ensued.

[4] In deciding HoneyBadger's summary judgment application, the judge found that "[t]here can be no doubt in these circumstances that Mr. Bue's naivete and ignorance is at the heart of this fraud" (*Judgment* at para 44), and that "[b]ut 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" (at para 45). Nonetheless, the judge held that, if HoneyBadger had complied with the instruction-verification processes under the PAD agreement by issuing a "password or security code or signature equivalent", the fraud loss would

have been avoided. In short, she concluded that, while Mr. Bue had actively cooperated in the fraud, HoneyBadger had failed to prevent the resulting loss and, therefore, both parties were equally responsible for that loss. In the result, she found Mr. Bue liable for $40,000 of the loss that he admitted to personally authorising, and that both had equally contributed to the remaining $200,000 loss. Therefore, she awarded $100,000 to Mr. Bue and $140,000 to HoneyBadger.

[5] Since Mr. Bue's cross-appeal questions the validity of the Bitcoin transactions, I address it first, concluding that the cross-appeal must be dismissed because there is no reason to suspect that the judge erred by finding that the transactions had occurred pursuant to valid agreements.

[6] I would allow HoneyBadger's appeal principally on the ground that the judge erred in law and in mixed fact and law when she attributed liability for the fraud loss to HoneyBadger. Her reasoning was incorrectly sourced from an inapplicable civil law principle under the *Civil Code of Québec*, CQLR c CCQ-1991, that is inconsistent with common law principles. As well, she misinterpreted the PAD agreement leading her to erroneously find that HoneyBadger had failed to comply with its terms.

[7] When the appropriate common law principles are applied to the facts as found by the judge, I conclude that HoneyBadger is entitled to the $200,000 now held by the Court of King's Bench. I would therefore set aside the *Judgment* and direct the local registrar in Swift Current to release the funds held by that Court to HoneyBadger, if Mr. Bue does not appeal from this result within the 60-day period for doing so. I would also award HoneyBadger costs of the summary judgment application, the appeal and the cross-appeal.

II. BACKGROUND

[8] Sometime in 2022, Mr. Bue invested online in what he believed was a company called "Main Bit Ltd.", unaware that it was not a legal entity. When he attempted to withdraw his investment, the company stopped responding to him.

[9] A short while later, someone ostensibly working for the "Ministry of Justice at the United Kingdom" contacted Mr. Bue to advise him that the Ministry had taken control of the assets of "Main Bit Ltd." with the intention of compensating investors like him. He was told he had to

transfer cryptocurrency to the Ministry before he would receive any compensation, and he made those payments but did not receive any compensation.

[10] Then, someone apparently from a "Cybercrime agency" named "Funds Recall" contacted Mr. Bue and offered to help him recover both his investment in "Main Bit Ltd." and the cryptocurrency he had transferred to the "Ministry of Justice at the United Kingdom". He was told that "Funds Recall" required a transfer of cryptocurrency before it could begin to assist him. Mr. Bue did not make those payments.

[11] However, the supposed "cybersecurity division" of the "FBI" then reached out to Mr. Bue, offering to assist him in recovering all the funds that he had transferred to the fraudsters in exchange for an $80,000 fee payable in cryptocurrency.

[12] On April 25, 2023, Mr. Bue contacted HoneyBadger to facilitate the purchase of $80,000 in Bitcoin. This was HoneyBadger's first interaction with Mr. Bue, and he did not make them aware of the earlier frauds or the reasons for the Bitcoin purchase. HoneyBadger sent Mr. Bue an email explaining the purchase process. Mr. Bue accepted the terms offered by HoneyBadger. In contemplation of an initial purchase, Mr. Bue completed and returned the PAD agreement and provided HoneyBadger with two email addresses as part of its know-your-client verification process. One of those email accounts (and its password) had been created and given to Mr. Bue by the third party posing as the "FBI".

[13] Using one of the email accounts he had provided, Mr. Bue instructed HoneyBadger to purchase Bitcoin totalling $79,991 in two transactions. The first was paid via wire transfer on April 27, 2023. The second was paid on May 1, 2023, by debiting Mr. Bue's credit union account under the PAD agreement. Mr. Bue acknowledges that he authorised these transactions.

[14] On May 29, 2023, HoneyBadger received emailed instructions to make a $10,000 purchase of Bitcoin and, the next day, another $30,000 worth. Mr. Bue acknowledges that he authorised these two purchases.

[15] HoneyBadger then received emailed requests for $100,000 of Bitcoin on each of May 31 and June 1, 2023. Mr. Bue says that he did not authorise these last two purchases.

[16] Each of the six Bitcoin purchase transactions arranged through HoneyBadger was initiated under an email that HoneyBadger received from an email account that Mr. Bue had provided to it for that purpose.

[17] Prior to these transactions occurring, Mr. Bue had granted the third party posing as the "FBI" remote access to his computer and had given the third party the password to the personal email account he used when purchasing Bitcoin. As mentioned, the third party had itself generated the other email account that Mr. Bue had told HoneyBadger was his own email. Critically, Mr. Bue instructed HoneyBadger to deposit the purchased Bitcoin into the third party's cryptocurrency wallet. At no time was HoneyBadger aware that Mr. Bue had been defrauded in the recent past, did not have exclusive control over or supervision of his email accounts, and did not own or control the wallet.

[18] On June 6, 2023, Mr. Bue objected to the last four Bitcoin transactions totalling $240,000. At that time, he asked his credit union to reverse the four debits on his account that were associated with those purchases, also totalling $240,000, debits which HoneyBadger had made under the PAD agreement.

[19] Once the credit union reversed the debits, HoneyBadger obtained an order ensuring that the $240,000 the credit union had taken back would be preserved (see *HoneyBadger Enterprises Ltd. v Bue and Innovation Credit Union*, 2023 SKKB 193). Proceedings against the credit union were later discontinued, and HoneyBadger's counsel held the preserved funds in trust pending the outcome of this litigation. When the *Judgment* was issued, $40,000 of the $240,000 was released to HoneyBadger since Mr. Bue had acknowledged authorising Bitcoin transactions in that amount. Following an application under Rule 15 of *The Court of Appeal Rules (Civil)*, I ordered HoneyBadger's counsel to pay the remainder of the preserved funds into court (see *HoneyBadger Enterprises Ltd. v Bue* (28 November 2025), Regina CACV4635 (SKCA)). The appeal and cross-appeal are about the parties' entitlement to the remaining $200,000, which is now held by the Court of King's Bench in the judicial centre of Swift Current.

III. *JUDGMENT*

[20] HoneyBadger, in its summary judgment application, argued that Mr. Bue had breached the PAD agreement by reversing the payments for Bitcoin purchases. It asserted that it had complied with guidelines prescribed by the Financial Transactions and Reports Analysis Centre of Canada [FINTRAC]. It denied responsibility for the fraud by the third party. HoneyBadger sought recovery of the full $240,000 that Mr. Bue owed to it for the Bitcoin purchase transactions.

[21] Mr. Bue, in his defence, claimed the two $100,000 transactions were unauthorised and had been initiated by fraudsters. He alleged that the PAD agreement required HoneyBadger to implement safeguards against that type of fraud, which it had failed to do. Mr. Bue also asserted that HoneyBadger had failed to comply with FINTRAC guidelines and was liable to him under *The Sale of Goods Act*, RSS 1978, c S-1. He counterclaimed for damages he alleged had resulted from the issuance of the preservation order.

[22] In her *Judgment*, the judge rejected Mr. Bue's arguments under *The Sale of Goods Act*, holding that cryptocurrency is not a *good* under that Act and finding that the transactions were supported by written agreements. She held that she did not have sufficient evidence to make a conclusive determination about whether HoneyBadger had complied with FINTRAC guidelines. The judge also dismissed Mr. Bue's argument that the preservation order had been obtained through an abuse of process, saying it was not inappropriate for HoneyBadger to seek a legally available remedy.

[23] As to their respective liability for the $240,000 fraud loss, the judge found that both parties bore responsibility. Mr. Bue, because he was careless in allowing fraudsters access to his computer and email accounts, which had actively enabled the "FBI" to make the unauthorised transactions. HoneyBadger, because it had failed to comply with the PAD agreement by not issuing a "password or security code or signature equivalent", which could have prevented the fraud.

[24] In the result, the judge awarded HoneyBadger $140,000 of the preserved funds and Mr. Bue $100,000. She dismissed Mr. Bue's counterclaim of abuse of process. She made no award of costs.

IV. ISSUES AND ANALYSIS

[25] As mentioned, it is appropriate to address the issue in Mr. Bue's cross-appeal first because it asks whether the Bitcoin purchase transactions were, of themselves, valid agreements under contract law. If they were invalid, it would be arguable as to whether HoneyBadger had any claim to the preserved funds. Following that, I discuss only those issues raised by HoneyBadger's appeal that allege error in the judge's analysis in the *Judgment* when attributing liability as between the parties.

A. Validity of the Bitcoin purchase agreements

[26] Mr. Bue alleges that the judge erred because she did not appreciate that there were no valid contracts between him and HoneyBadger for the purchase of Bitcoin. He says the parties never reached *consensus ad idem* because he had not objectively manifested an intention to be bound by the two $100,000 transactions (citing *Saint John Tug Boat Co. v Irving Refinery Ltd.*, [1964] SCR 614). He made this same argument before the judge in the summary judgment application.

[27] The judge found that Mr. Bue had agreed in email correspondence (which the judge held had formed a valid contract) to acquire cryptocurrency from HoneyBadger through a transactional process that he could initiate by email and pay for through a pre-authorised debit made under the PAD agreement. She called this the "Transaction Agreement". However, she also held that each transaction was itself a "separate agreement", describing the contracting process in these terms:

> [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.

[28] Each Bitcoin purchase transaction under the Transaction Agreement followed this pattern:

(a) by email, Mr. Bue (or whoever had access to his email account) would direct HoneyBadger to purchase a certain dollar amount of cryptocurrency;

(b) by issuing a PAD instruction under the PAD agreement, HoneyBadger would instruct Mr. Bue's credit union to debit funds in the requested amount from Mr. Bue's credit union account;

(c) once it had received the debited funds from the credit union, HoneyBadger would advise Mr. Bue by email of the then current market rate for the cryptocurrency he had requested;

(d) when Mr. Bue received a price quote from HoneyBadger, he would confirm by email his acceptance of the amount of cryptocurrency offered in the quote and confirm that it was to be deposited to the wallet address he had given to HoneyBadger; and

(e) upon receiving the transaction confirmation from Mr. Bue, HoneyBadger would process the purchase transaction and deposit the cryptocurrency into the wallet Mr. Bue had provided for that purpose.

[29] I do not understand Mr. Bue to take issue with the judge's finding that the Transaction Agreement was a valid contract. Therefore, if the judge's findings that the Transaction Agreement was a valid contract and that "each transaction was a separate agreement" are undisturbed, it stands as a fact that Mr. Bue agreed that he would enter contractually binding arrangements with HoneyBadger for the purchase of Bitcoin in accordance with the terms of the Transaction Agreement. Critically, the judge found that the Bitcoin transactions had all occurred in accordance with the *ad idem* terms of that agreement — i.e., over email and under the PAD agreement. In this context, there is no question about whether Mr. Bue intended to be bound to pay the purchase price for Bitcoin transactions that occurred under the terms of the Transaction Agreement. He says, rather, that the judge erred because the parties had not formed valid contracts for the two $100,000 fraudulent transactions since:

(a) he had no knowledge of the transactions when they occurred;

(b) the transactions were initiated by an unauthorised third party who had gained access to his email account; and

(c) he did not receive any benefit from the transactions as the Bitcoin was deposited into the fraudster's wallet.

While these facts are not disputed, they do not support a finding of palpable error in the judge's conclusion that the Bitcoin purchase transactions were made under valid contracts. I say so for four reasons.

[30] As to the first reason, nothing in the parties' contractual arrangement prevented Mr. Bue from delegating specific tasks or responsibilities to another person while maintaining overall accountability under the Transaction Agreement and the PAD agreement. Mr. Bue has not pointed to anything in the law of contract, in the Transaction Agreement, or on the record to support his contention that the fact he lacked knowledge of those online transactions as they were occurring somehow negated their validity. Related to this point, while I fail to see how his second reason could affect contract formation, the third party posing as the "FBI" did not *gain access* to Mr. Bue's computer and email account; *he voluntarily gave the "FBI" that access*. Importantly, Mr. Bue did not claim that HoneyBadger owed him a duty of care in contract or at common law to protect him from himself. Respectfully, there is no cogency to the arguments that effectively assert that Mr. Bue should be relieved of liability for the self-induced fraud loss because his own carelessness had caused it.

[31] Thirdly, the fact that Mr. Bue did not receive any Bitcoin himself does not establish an absence of the consideration necessary to form a binding contract, which I assume is the basis for this argument. The fact a third party obtains the full benefit of an agreement does not of itself render that contract invalid, although it might give rise to an issue of privity if the third party sought to enforce it (see, e.g., *Fraser River Pile & Dredge Ltd. v Can-Dive Services Ltd.*, 1999 CanLII 654, [1999] 3 SCR 108 (SCC)). There is no merit to this argument on the issue of contract validity.

[32] Lastly, it is relevant to all three of these arguments that the law of agency permits an agent to enter contracts on behalf of an undisclosed principal or third-party beneficiary. While FINTRAC guidelines address financial arrangements made on behalf of undisclosed beneficiaries, the judge held that the evidence did not support Mr. Bue's contention that HoneyBadger had failed to comply with those requirements. Further, even if HoneyBadger had failed to comply as Mr. Bue alleged,

I would be hard pressed to find that that failure had affected the parties' satisfaction of the steps necessary to form a valid contract.

[33] In short, Mr. Bue has not raised a sufficient case to conclude that the judge erred when she held that the Bitcoin transactions had occurred under valid contracts.

B. Allocation of liability for the fraud loss

[34] In its appeal, HoneyBadger asserted that the judge's decision to allocate part of the loss resulting from the fraud to it was without proper legal foundation. That is, it says there is no applicable legal principle supporting her decision in that regard. Given the facts as found by the judge, I agree.

[35] HoneyBadger acknowledges that the judge cited the correct common-law principle for allocating a loss between two innocent parties in a fraud case, as stated by the Ontario Court of Appeal in *Isaacs v Royal Bank of Canada*, 2011 ONCA 88 [*Isaacs*]. Notably, the principle in *Isaacs* does not call for a relational approach to liability for a fraud loss based on each innocent party's relative inattentiveness or recklessness. The issue under the *Isaacs* principle is whether the carelessness of an innocent party actively enabled the fraud to occur, as opposed to whether the innocent party was simply an uninvolved victim of it.

[36] In *Isaacs*, the appellant was an innocent party because she had not committed the fraud. She had facilitated it, however, by choosing to grant a mortgage to a bank to secure a stranger's borrowings. When the stranger disappeared with the borrowed funds, the appellant argued that the bank was in a better position than her to detect the fraud and, therefore, it ought to be held responsible for the loss. The Ontario Court of Appeal rejected that argument and upheld the trial court's ruling that the appellant was solely responsible for the loss, writing:

> [3] … A simple review by the Bank of the mortgage documents submitted by or on behalf of the appellant could not and did not reveal any prospect of fraud to the Bank. In sharp contrast, as the motion judge found, had the appellant taken the simple precaution of reading the many documents she signed, the fraudulent nature of the mortgage transaction would have been immediately apparent. There was ample evidence on this record to support the motion judge's finding that the appellant was in the best position to detect and prevent the fraud.
>
> [4] Moreover, contrary to the appellant's submission, this is not a case involving two equally innocent parties. The appellant was not entirely innocent of any wrongdoing. She

> agreed to serve as an accommodation mortgagor for a stranger, for compensation, without disclosure to the Bank of the nature of the transaction.
>
> [5] The motion judge found that, in so doing, the appellant "assisted the fraudsters to perpetuate the fraud even if she did not know the particulars of the transaction". This finding was open to the motion judge on the evidence.
>
> [6] 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, 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 bear the burden of the loss.
>
> (Emphasis added)

[37] In the trial decision in *Isaacs v Royal Bank of Canada*, 2010 ONSC 3527, the motions judge had made the following findings about the bank's ability to detect the fraud:

> [44] In short, the Bank was entitled to rely on the documents signed by Ms Isaacs. It had no obligation to investigate the background and no obligation to ensure Ms Isaacs understood the transaction. Although the Bank could certainly have been more careful in protecting its own interests, it had no duty to Ms Isaacs to do so and no responsibility to protect the interests of Ms Isaacs. A failure by the Bank to detect the fraud does not excuse Ms Isaacs from her liability when it was apparent on its face on the documents Ms Isaacs signed and provided to the Bank – a fact that would be known to Ms Isaacs if she had read them, but would not have been known to the Bank.

[38] The Court in *Isaacs* distinguished the decision in *Marvco Colour Research Ltd. v Harris*, 1982 CanLII 63, [1982] 2 SCR 774 (SCC) [*Marvco*], even though Estey J. found a similar principle in the context of the defence of *non est factum*, writing for the unanimous Court (at 785-786):

> In my view, with all due respect to those who have expressed views to the contrary, the dissenting view of Cartwright J. (as he then was) in *Prudential, supra*, correctly enunciated the principles of the law of *non est factum.* In the result the defendants-respondents are barred by reason of their carelessness from pleading that their minds did not follow their hands when executing the mortgage so as to be able to plead that the mortgage is not binding upon them. The rationale of the rule is simple and clear. As between an innocent party (the appellant) and the respondents, the law must take into account the fact that the appellant was completely innocent of any negligence, carelessness or wrongdoing, whereas the respondents by their careless conduct have made it possible for the wrongdoers to inflict a loss. As between the appellant and the respondents, simple justice requires that the party, who by the application of reasonable care was in a position to avoid a loss to any of the parties, should bear any loss that results when the only alternative available to the Courts would be to place the loss upon the innocent appellant. In the final analysis, therefore, the question raised cannot be put more aptly than in the words of Cartwright J. in [*Prudential Trust Co. v Cugnet*, [1956] SCR 914 at p. 929]: "... which of two innocent parties is to suffer for the fraud of a third." The two parties are innocent in sense that they were not

> guilty of wrongdoing as against any other person, but as between two innocent parties there remains a distinction significant in law, namely that the respondents, by their carelessness, have exposed the innocent appellant to risk of loss, and even though no duty in law was owed by the respondents to the appellant to safeguard the appellant from such loss, nonetheless the law must take this discarded opportunity into account.
>
> (Emphasis added)

[39] In this appeal, HoneyBadger submits that the judge ignored the *Isaacs* principle in her reasoning and instead based her decision on inapplicable principles of civil law under the *Civil Code of Québec*. Albeit that it was erroneous, I find her reasoning on the issue of liability was not as straightforward as that.

[40] In the *Judgment*, the judge relied on the common law decision in *Bank of Montreal v Asia Pacific International Inc.*, 2018 ONSC 4215, which involved a wire-transfer fraud. She observed that the Court in *Asia Pacific* had itself referred to the decision in *Rogers v Priyance Hospitality Inc.*, 2016 ONSC 7851, where the plaintiff had argued a principle from *Marvco*. In her reasons in the *Judgment*, the judge embraced the summary by the Court in *Asia Pacific* of the principle the plaintiff in *Rogers* had found in *Marvco*, which was: "as between two innocent parties, justice requires that the party who was in a position to prevent the loss should bear it" (*Asia Pacific* at para 38). However, as noted, Estey J. held in *Marvco* that, as between an innocent party and a careless party, the law accounts for the fact that the latter, "by their careless conduct, made it possible for the wrongdoers to inflict a loss".

[41] Moreover, in her liability analysis, the judge did not address the fact that the Court in *Isaacs* had distinguished *Marvco* (articulating a more focussed rule) on the basis that that case had involved the carelessness of two innocent victims *one* of which who had been careless, whereas the role of one of the two innocent parties in *Isaacs* "was more than careless. It involved affirmative action on her part *that facilitated the fraud*" (at para 6, emphasis added). The Court in *Isaacs* ruled that, "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 bear the burden of the loss" (at para 7, emphasis added). Respectfully, the facts of *Isaacs* are the circumstances of this case as found by the judge and, therefore, she had to address both the applicable dicta of *Marvco* and that similar facts had led the Court in *Isaacs* to "distinguish" *Marvco* by identifying a rule for allocating liability that was even truer to the facts before her.

[42] Moreover, the judge appears to have understood that the facts she had found were aligned with those of *Isaacs* because she wrote:

> [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.
>
> (Emphasis added)

[43] Her conclusion about Mr. Bue bearing liability for the first four transactions is in accordance with the *Isaacs* principle. And, respectfully, that "line" of liability was just as "clear with respect to the $200,000 purchases of which he was unaware" (at para 52). The judge's findings of fact make this plainly evident:

> [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.
>
> (Emphasis added)

[44] Regardless, having decided that "the line was less clear" with respect to the two $100,000 transactions (at para 52), the judge erroneously allocated liability for those losses as between Mr. Bue and HoneyBadger under a civil law principle, which she drew from the decision in *Alfagomma Inc. v HSBC Bank Canada*, 2022 QCCS 3655 [*Alfagomma*]. This error of law requires some explanation.

[45] In the concluding paragraphs of her reasoning in the *Judgment* on the issue of liability allocation, the judge reconfirmed that, but for Mr. Bue's incomprehensible active participation in the fraud, it would not have occurred. Nonetheless, relying on *Alfagomma*, she split the liability for the two $100,000 transactions equally between HoneyBadger and Mr. Bue, writing:

> [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: [quoted text omitted]
>
> [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, Alfagomma'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.

[46] To explain why it was a legal error for the judge to follow the reasoning in *Alfagomma*, it is necessary to understand the basis for the ruling in that case. The issue in *Alfagomma* was whether a bank had exercised reasonable prudence when transacting wire transfers that turned out to be fraudulent. Citing a text on the civil code (J Beaudoin, Patrice Deslauriers et Benoît Moore, *La responsabilité civile*, 9th ed, vol. 2, Montréal, Éditions Yvon Blais, 2021, p 485-486, § 2-432) as authority for the proposition, the Québec Court remarked that "[a] bank's most basic duty to its client is to execute its instructions without interfering in a client's internal affairs. However, by its nature, *the banking contract implies a duty to act with reasonable prudence and diligence*" (*Alfagomma* at para 84, emphasis added). The Québec Court noted that the fulfilment of this duty requires banks to "exercise a certain degree of care to protect their clients from fraud, especially in the face of suspicious activity" (at para 85). In support of this principle, the Court referred to and quoted from Nicole L'Heureux et Marc Lacoursière, *Droit bancaire*, 5th ed, Montréal, Éditions Yvon Blais, 2017, at para 286, where the authors wrote that a bank "n'a pas à faire de

recherche au-delà de son mandat ou du chèque qui est devant elle, à moins d'avoir connaissance de circonstances suspectes", which I would unofficially translate as meaning that a bank does not have to conduct any research beyond the scope of its mandate or the cheque in front of it, unless it has knowledge of suspicious circumstances.

[47] However, the Québec Court in *Alfagomma* had also referred to the decision in *124329 Canada inc. v Banque Nationale du Canada/National Bank of Canada*, 2011 QCCA 226 [*Jackson*], where Kasirer J.C.A. (as he then was) discussed how "a banker's duty of prudence is understood in the context of their duties of non-interference" (*Alfagomma* at para 86). In *Jackson*, Kasirer J.C.A. explained:

> [66] There is a consensus in the decided cases and among scholars in Quebec that the general extracontractual duty set forth at article 1457 C.C.Q. is the proper measure of a bank's conduct in respect of its duty to third parties. The intensity of this obligation is one of means such that, in the civil law, a bank must take reasonable measures to avoid causing a loss to others, including third parties. When one of its customers undertakes transactions that the reasonable banker in the circumstances would consider to be suspicious, the bank must take appropriate measures to remove the suspicion in order to prevent misdealing in the account that would harm third parties. Failure to take such measures, such as suspending a transaction while its correctness is verified, may result in liability to those who suffer a loss as a result. …
>
> [67] Yet the intensity of the obligation must be understood in the context of legitimate institutional practices of non-intervention in account holders' affairs in the banking industry. In particular, the content of the obligation must take into account the absence of a duty on banks to see to the performance of fiduciary-type obligation for trust accounts. Accordingly, courts should be careful not to deem a bank to have knowledge of misdealing too readily. <u>While the standard of conduct imposed on banks under article 1457 C.C.Q. is perforce measured objectively, it is appropriate to look for strong signs of misdealing before deciding a bank can be held liable for not having taken measures to prevent it.</u> <u>Not only would too low a standard impose untenable transactions costs on banks, it would set Quebec law out of step with authorities elsewhere in the country when the transactions in question are not substantively different or easier to police</u>.
>
> (Emphasis added)

[48] I draw two conclusions from the quoted parts of Kasirer J.C.A.'s reasons in *Jackson*. The first is that the principle upon which the judge in this case relied when attributing liability to HoneyBadger is grounded in a civil law duty of care that banks (and everyone else) in Québec owe under Article 1457 of the *Civil Code of Québec*, which reads as follows:

> 1457. Every person has a duty to abide by the rules of conduct incumbent on him, according to the circumstances, usage or law, so as not to cause injury to another.

> Where he is endowed with reason and fails in this duty, he is liable for any injury he causes to another by such fault and is bound to make reparation for the injury, whether it be bodily, moral or material in nature.
>
> He is also bound, in certain cases, to make reparation for injury caused to another by the act, omission or fault of another person or by the act of things in his custody.

[49] Second and more critically, Kasirer J.C.A. understood that the civil law principle codified in Article 1457 of the *Civil Code of Québec* and applied in *Alfagomma* was "out of step with authorities elsewhere in the country" (at para 67). One of those authorities is, quite plainly in my opinion, *Isaacs* and another is *Marvco*.

[50] Moreover, even if the civil law principle in *Alfagomma* for attributing liability to a bank was applicable in this case (which Kasirer J.C.A. said should require "strong signs of misdealing"), it was not met on the facts found by the judge in the *Judgment*, most notably:

> [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. …
>
> (Emphasis added)

[51] To sum up, Article 1457 of the *Civil Code of Québec* does not apply in Saskatchewan and, even if principles equivalent to it could be found in the common law, those principles are not engaged on the facts of this matter. Furthermore, the principle articulated in *Isaacs* contradicts the existence of a common law duty of care in these circumstances. And, in any event, Mr. Bue did not plead that HoneyBadger owed him some type of duty of care.

[52] As such, I conclude that the judge erred in law by applying a principle taken from the *Civil Code of Québec* in these circumstances. For this reason alone, the *Judgment* must be set aside.

C. Compliance with the PAD agreement

[53] Although I would set aside the *Judgment* based on the foregoing error of law, the judge's allocation of liability for the fraud loss also rested in part on her conclusion that HoneyBadger had failed to comply with the terms of the PAD agreement and that, if it had complied, the fraud could

have been avoided. In its appeal, HoneyBadger submits that the judge palpably erred in her interpretation of clause 8 of that agreement when she reached that conclusion. I agree.

[54] As noted earlier in these reasons, the judge rejected Mr. Bue's argument that HoneyBadger had failed to comply with FINTRAC guidelines regarding the "travel rule" (an anti-money laundering regulation), which he had said could have prevented the fraud loss. She did so because there was no expert evidence to support a finding that HoneyBadger was in breach of that rule (she said there was no expert evidence proving that it had complied with the rule either). The judge then wrote:

> [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.
>
> (Emphasis added)

[55] The judge's conclusion – that HoneyBadger was liable because it failed to comply with the PAD agreement – results from an interpretation error about what is required by the second sentence of clause 8 of that agreement. Clause 8 of the PAD agreement states:

> 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.
>
> (Emphasis added)

[56] Notably, the judge does not appear to have conducted a principled interpretation of the PAD agreement or clause 8 in accordance with the approach in *Sattva Capital Corp. v Creston Moly Corp.*, 2014 SCC 53. Under *Sattva*, contract interpretation is an exercise in which the principles of interpretation are applied to the words of the written agreement, typically considered in light of the factual matrix of contract formation. The goal of interpretation is to ascertain the objective intentions of the parties to a contract. Importantly, in *Sattva* (at para 47), Rothstein J. quoted from *Reardon Smith Line Ltd. v Hansen-Tangen*, [1976] 3 All ER 570 (HL), where Lord

Wilberforce had described the factual matrix surrounding the making of a commercial agreement (at 574):

> No contracts are made in a vacuum: there is always a setting in which they have to be placed. …In a commercial contract it is certainly right that the court should know the commercial purpose of the contract and this in turn presupposes knowledge of the genesis of the transaction, the background, the context, the market in which the parties are operating.

[57] Here, the judge seems to have misunderstood the PAD agreement to be an arrangement between HoneyBadger and Mr. Bue for the benefit of Mr. Bue, whereas the PAD Agreement *appears* to be a standard-form contract used by credit unions to address their obligations and liabilities and those of third-party payees, like HoneyBadger, in circumstances where a credit union's customer, like Mr. Bue, pre-authorises the third party to make automated electronic debits from the customers' credit union accounts. Neither party made that argument before the judge or this Court, but the standard-form nature of the PAD agreement is supported by the copyright notice on the bottom of the first page, which asserts that copyright in the preprinted form is owned by "Central 1 Credit Union". The beneficiaries of the contract terms are confirmed in the signature block of the form, where it states that "this agreement is provided for the benefit of the "Payee" [i.e., HoneyBadger] and "Processing Institution" [i.e., Mr. Bue's credit union]". And, at the top of the first page of the agreement, the Processing Institution instructs the Payee how to process a PAD. Nevertheless, the parties argued this matter as though the PAD agreement was subject to the *Sattva* approach, and the judge interpreted it in a matrix of factual circumstances relevant to the formation of a contract between HoneyBadger and Mr. Bue only.

[58] Regardless of how it is approached, the judge's errors are in palpably misunderstanding the commercial purpose of the PAD agreement by overlooking the fact that the credit union was a party to it and in missing the fact that the credit union and HoneyBadger were the beneficiaries of its terms. These errors led the judge to the wrong interpretive conclusions about what the parties' objective intentions were with respect to the requirements of clause 8. As it relates to the facts of this matter, these errors are readily evident and override the judge's interpretation. They are also legal errors — i.e., the failure to apply the correct principles and the failure to consider a relevant factor — that likewise invalidate the judge's interpretation.

[59] The errors and their effect on the judge's interpretation are manifest in her description of what clause 8 of the PAD agreement required. The interpretation exercise in this case was comprised of rejecting HoneyBadger's subjective avowals, and accepting Mr. Bue's subjective claims, about what that clause required. The judge did not interpret clause 8 herself or attempt to ascertain the objective intentions of the parties to the PAD agreement, one of which – the credit union – was no longer a party to the litigation. This is evident from her description of the requirements of clause 8, which exhibits a misunderstanding about who had generated that contract, why it was generated and who benefited from it:

> [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: [text of clause 8 omitted]
>
> [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 [a representative of HoneyBadger] 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.
>
> [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.
>
> (Emphasis added)

[60] Respectfully, if the commercial purpose and context of the PAD agreement and its other terms and conditions had been brought into the interpretation exercise, it would have been plainly evident – for example – why the credit union had debited Mr. Bue's account in these circumstances. It did so because, under the "clear wording of the PAD Agreement", the credit union had no obligation to Mr. Bue to monitor his account, to verify his debit transactions or to supervise the automated PAD process. To the credit union, the purpose of the PAD agreement was to limit its obligations and liabilities.

[61] Because the judge's interpretation results from palpable and overriding error and is otherwise invalid, clause 8 of the PAD agreement must be re-interpreted. Recall, the most relevant text in question states: "I/We agree 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" (emphasis added). The germane parts being in the passive voice ("will be issued" and "will constitute valid authorization"), I find there is an initial ambiguity about *who* will issue the "password or security code or other signature equivalent", although there are just three possibilities: HoneyBadger, Mr. Bue and the credit union.

[62] To begin resolving that ambiguity, I observe that there is no doubt about to whom or to what four identifying terms are referring in the PAD agreement:

(a) the term *Processing Institution* refers to Mr. Bue's credit union because, in the box on the front page of the PAD agreement entitled "Payor Financial Institution Name and Address *(the 'Processing Institution')*" (italics in original), Mr. Bue handwrote: "Innovation Credit Union Cabri Sask S0N0J0";

(b) the term *Payee* refers to HoneyBadger, as it had typed its identifying information into the box entitled "Payee Name (the 'Payee')";

(c) Mr. Bue is the *Payor* because he handwrote his name and postal address in the boxes marked for "Account Holder Name(s) (the 'Payor') *(last name or business name, first name)*" (italics in original); and

(d) the phrase *the Account* refers to Mr. Bue's account with his credit union, the details of which are handwritten in the box entitled "Payor Account *(the Payor's account at the Processing Institution; the 'Account')*" (italics in original).

[63] The notations of *I/we* and *me/us* in the PAD agreement also refer to Mr. Bue. The signature box of the PAD agreement, where only Mr. Bue was required to sign to signify his acceptance of that agreement, leaves me with no hesitation in reaching that conclusion:

> I/We acknowledge that this agreement is provided for the benefit of the "Payee" [i.e., HoneyBadger] and "Processing Institution" [i.e., the credit union] and is provided in consideration of the Processing Institution agreeing to process debits ("PADs") against the Account with the Processing Institution in accordance with the Rules of the Canadian Payments Association (the "CPA Rules").
>
> By signing this agreement, the Payor [i.e., Mr. Bue] acknowledges having received and having read a copy of this agreement, including the terms and conditions on page 2, acknowledges understanding the terms and conditions of this agreement, and agrees to be bound by the terms and conditions of this agreement, including the terms and conditions on page 2.
>
> I/We warrant and guarantee that the person(s) whose signature(s) required to sign on the Account have signed the agreement.
>
> x *[Mr. Bue's signature]* *[April 28/23, handwritten]*
>
> Payor Signature Date

[64] With those terms defined or understood, the text of clause 8 that requires interpretation in this matter states: "[Mr. Bue agrees] a password or security code or other signature equivalent will be issued and will constitute valid authorization for the [credit union] to debit [his account]." That interpretation suggests, but does not confirm, that Mr. Bue is the one who would issue the security item — i.e., the password, security code or other signature equivalent — that "will constitute valid authorization" for his credit union to debit his account with them.

[65] Since some uncertainty remains about who the parties intended would issue the security item, resort must be had to the text in the first sentence of clause 8. The first sentence states that, because he had pre-authorised HoneyBadger to issue "PADs with sporadic frequency", "[Mr. Bue understands] that [HoneyBadger] is required to obtain an authorization from [him] for each and

every PAD prior to the PAD being exchanged and cleared". This interpretation of the first sentence stands to reason because Mr. Bue did not set up pre-authorised monthly debits of his credit union account in a fixed amount with respect to which he could have collectively granted permission under a single authorisation (as one might do to automate monthly car-loan payments). He pre-authorised HoneyBadger to debit his account whenever he instructed them to do so and in whatever amount he told them – i.e., "with sporadic frequency". And, since it was Mr. Bue's credit union account and his money in it, no one else was entitled to authorise HoneyBadger and the credit union to debit his account.

[66] Therefore, to paraphrase the authorisation process, an authorisation to debit Mr. Bue's credit union account had to travel from Mr. Bue to HoneyBadger each time he instructed HoneyBadger to debit funds from that account. However, there is no mention in the PAD agreement of how it must travel.

[67] At this point of the interpretation exercise, the importance of the commercial purpose of a PAD agreement comes into focus. Once Mr. Bue had authorised HoneyBadger to debit his credit union account, HoneyBadger would notify his credit union of that fact under a "PAD", which would cause the credit union to debit Mr. Bue's account. The contractual meaning of the acronym *PAD* is found in the instructions to HoneyBadger (as the Payee) about how to issue a PAD. The instructions at the top of the first page of the PAD agreement state:

> INSTRUCTIONS
>
> 1. The Payee must retain this agreement for at least 12 months after the last Pre-Authorized Debit (PAD) is issued.
>
> 2. The Payee can obtain the Transaction Type Code from the Payments Canada website See CPA Rule 005, Standards for the Exchange of Financial Data on AFT Files (Section D, Appendix 2, Transaction Types).
>
> 3. The Payee will insert the number of days required to cancel a payment in the "Cancel Payment" Section (cannot exceed 30 days).

In addition, in the box marked "Description of PAD *(optional)*" (italics in original), HoneyBadger had inserted: "Purchase of cryptocurrency from HoneyBadger Enterprises Ltd."

[68] In technical terms, each PAD would include a numerical code that identified the type and purpose of the automated funds transfer (AFT) in question under Rule 005 of the Canadian Payments Association, "Standards for the Exchange of Financial Data on AFT Files" (2026)

https://www.payments.ca/sites/default/files/standard005eng.pdf, without which the transfer cannot be processed. In addition to a code, an AFT file includes institution and account information and the amount to be credited or debited, as the case may be.

[69] On this basis, HoneyBadger is evidently the party who would issue a PAD, and once issued, the PAD would initiate an automated transfer of funds from Mr. Bue's credit union account to HoneyBadger's account, i.e., without the credit union's active involvement. This is confirmed by clause 9 of the PAD agreement, which addresses the credit union's obligation to verify PADs by stating: "[Mr. Bue acknowledges] that the [credit union] is not required to verify that a PAD has been issued in accordance with the particulars of this agreement, including, but not limited to, the amount". Clause 10 states: "[Mr. Bue acknowledges] that the [credit union] is not required to verify that any purpose of payment for which the PAD was issued has been fulfilled by [HoneyBadger] as a condition to honouring a PAD issued or caused to be issued by [HoneyBadger] on [Mr. Bue's credit union account]". When the commercial purpose of the agreement is taken into account, the text of these provisions is unambiguous in its meaning. The provisions were included in the PAD agreement to protect credit unions from being found liable to their customers, presumably because the electronic transfer of funds under a PAD instruction is an automated process.

[70] The authorisation in question is on the other side of this equation. Clause 8 states that a "password or security code or other signature equivalent will be issued" to authorise or allow all of that to occur on the PAD side. As clause 8 makes clear, that security item – when issued – "will constitute valid authorization for [Mr. Bue's credit union] to debit [his credit union account]". To be absolutely clear about this, the "password or security code or other signature equivalent" is what authorises HoneyBadger to issue a PAD to automatically debit Mr. Bue's credit union account and it thereby indirectly authorises the credit union to transfer funds from that account to HoneyBadger. The credit union is not involved with the debit-authorisation process and does not have to verify the validity of the resultant account-debiting. As such, there is no logic in concluding that the parties intended the credit union to issue a security item under clause 8.

[71] With that commercial and contractual background in place, I return to the text in question to address the remaining ambiguity about whether it was HoneyBadger or Mr. Bue who the parties intended would issue a security item as a valid authorisation for the debiting of Mr. Bue's account.

When placed in its appropriate context, the text of clause 8 on its face requires Mr. Bue to generate the "password or security code or other signature equivalent". That interpretation is consistent with a common-sense understanding of who typically generates a password or security code or adopts a signature equivalent – it is the individual who intends to rely on it for security or authentication purposes. The interpretation also logically fulfils the commercial purpose of the contract in the payments regime. Moreover, while they both benefited from its terms, neither the credit union nor HoneyBadger were required to execute the PAD agreement, only Mr. Bue. That is because only Mr. Bue had obligations under the PAD agreement. Neither of HoneyBadger (the Payee) or his credit union (the Payment Processor) were contractually required to do anything under any of its terms, including under clause 8 when properly interpreted. The PAD agreement protected them for acting on the instructions of their common client, Mr. Bue.

[72] Recall that the signature block of the PAD agreement states that Mr. Bue acknowledges that the agreement is "for the benefit of [HoneyBadger] and [his credit union] and is provided in consideration of [his credit union] agreeing to process debits ('PADs') against [his account with the credit union] *in accordance with the Rules of the Canadian Payments Association (the 'CPA Rules')*" (emphasis added). As HoneyBadger submitted in this matter, the rules of the Canadian Payment Association [CPA] provide that a payee must obtain an "Authorization" from the payor for each transaction that the payee places, a requirement which is reproduced as a contractual term in the first sentence of clause 8 of the PAD agreement.

[73] The CPA rules define the word *Authorization* as "the consent or agreement, in accordance with applicable law, of a Payor whose identity has been verified by Commercially Reasonable Methods, and 'Authorized' has a corresponding meaning". The term *Commercially Reasonable Methods* is itself defined to mean "procedures for verifying the Payor's identity (i.e. that the Payor is the person that they purport to be)" (Payments Canada, "Rule H1: Pre-Authorized Debits (PADS)" at Part 1 - General, s 5a and 5e (2025) https://www.payments.ca/sites/default/files/h1eng.pdf).

[74] Interpreted in accordance with the CPA Rules, the authorisation requirement in clause 8 of the PAD agreement is there to ensure that HoneyBadger has taken commercially reasonable steps to verify Mr. Bue's identity so that it could rely on his consent or agreement to debit his account

before it did so by issuing a PAD instruction to his credit union. There is no dispute that HoneyBadger had conducted a know-your-client verification process that verified Mr. Bue's identity (i.e., that he was who he purported to be), his physical address and his email accounts, cross-referenced with his government-issued identification. As the judge found: "HoneyBadger, at all times, believed it was dealing with Mr. Bue" (*Judgment* at para 45).

[75] Notably, under the CPA rules an *Authorization* is a payor's "consent or agreement, in accordance with applicable law". The second sentence of clause 8 adds some substance to the CPA requirements by indicating that the payor's authorisation of a PAD (i.e., their consent or agreement to it) "will be issued" in the form of "a password or security code or other signature equivalent". The word *password* and the term *security code* are common enough to be readily understood in and of themselves, but here the *ejusdem generis* principle of interpretation provides that they should be interpreted in this contract as two specific forms of a "signature equivalent".

[76] Although not mentioned in argument, *The Electronic Information and Documents Act, 2000*, SS 2000, c E-7.22, defines an *electronic signature* to mean "information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document" (s. 3(b)). Section 14 of that Act states that "[a] requirement pursuant to any law for the signature of a person is satisfied by an electronic signature". In *I.D.H. Diamonds NV v Embee Diamond Technologies Inc.*, 2017 SKQB 79, [2017] 9 WWR 172, aff'd 2017 SKCA 79, Layh J. held that the four elements of an electronic signature in the context of emails sent by a person are (at para 57):

> (1) The presence of some type of "information" on the emails;
>
> (2) Such information may be in electronic form;
>
> (3) The information must have been "created or adopted [by the person] in order to sign a document"; and
>
> (4) The information must be "attached to or associated with the document."
>
> (Emphasis added; bracketed information in original)

See also *Achter Land & Cattle Ltd. v South West Terminal Ltd.*, 2024 SKCA 115, where the majority and minority opinions, although disagreeing on other points, both affirm that an electronic signature must be created or adopted *by the person who uses it*.

[77] Therefore, based on the commercial purpose of the PAD agreement and how PADs function, the applicable CPA rules and provisions of *The Electronic Information and Documents Act, 2000*, and the text of clause 8 itself, that clause is most logically interpreted as follows:

> 8. If this agreement provides for PADs with sporadic frequency, Mr. Bue understands that HoneyBadger is required to obtain an authorization from him for each and every PAD prior to the PAD being exchanged and cleared by the credit union. Mr. Bue agrees that he will create or adopt a password or security code or other signature equivalent that will constitute his valid authorization of HoneyBadger to issue a PAD that instructs the credit union to debit his credit union account.

[78] Interpreted in this way, HoneyBadger did not fail to comply with the terms of the PAD agreement by failing to issue a "password or security code or other signature equivalent" to Mr. Bue for him to use when authorising HoneyBadger to debit his account with the credit union.

[79] Furthermore, considering the opposite scenario – i.e., where it was up to HoneyBadger to issue the security item that it could rely upon as its authority to debit Mr. Bue's account – leads to the conclusion that the issuance by HoneyBadger of "a password or security code or other signature equivalent" would not have avoided the fraud loss in the circumstances of this case.

[80] The two sets of purchase instructions to HoneyBadger to buy $100,000 of Bitcoin were emailed from Mr. Bue's personal email account. HoneyBadger responded by sending market-price quotes to that email account, advising that it would issue a PAD in the requested amount to debit Mr. Bue's account. HoneyBadger received another email from that email account accepting the quote and providing it with a cryptocurrency wallet address into which it was instructed to deposit the Bitcoin. HoneyBadger sent an email back acknowledging receipt of the cryptocurrency wallet's address. For the May 31, 2023, $100,000 transaction, HoneyBadger sent another email back noting that it was to deposit Bitcoin to the same wallet as it had the day before, referring to the May 30, 2023, $30,000 transaction, and it received an email back confirming that observation. HoneyBadger then purchased the quoted Bitcoin and deposited it into the identified wallet.

[81] I reach the secondary conclusion that the issuance of a security item would not have avoided the fraud loss because, if clause 8 had required HoneyBadger to generate and send Mr. Bue "a password or security code or other signature equivalent", then logic and the PAD agreement would dictate that Mr. Bue would have had to send it back to HoneyBadger to authorise each

debiting of his account. That makes sense, but it is not rational to conclude that this would have avoided the fraud loss.

[82] As noted earlier, there is no mechanism or pathway fixed in the PAD agreement for providing HoneyBadger with an authorisation. Since their relationship was not an in-person affair, presumably it could have been done in the same emails in which Mr. Bue had directed HoneyBadger to debit his account and to use the funds to acquire Bitcoin for him. This, of course, requires a distinguishment between the "valid authorisation", on the one hand, and the emailed direction to debit his account and buy Bitcoin, on the other – i.e., it assumes that the security code, password or other signature equivalent is something additional that he had to attach to or associate with the emailed instructions. However, since Mr. Bue had been previously defrauded three times and had then given the "FBI" unsupervised and unfettered access to his computer and to his email account *for the purpose of facilitating the Bitcoin purchases*, there is, respectfully, no reason to hope that he might not have given the "FBI" the "password or security code or other signature equivalent" that was necessary to pay for those purchases – regardless of whether he or HoneyBadger were contractually required to issue it.

[83] All of which is to say that the judge erred in her interpretation of the PAD agreement leading her to erroneously conclude that HoneyBadger had failed to comply with it. Even if she had not erred in her interpretation, there was no foundation in her factual findings to conclude that the fraud loss could have been avoided if HoneyBadger had complied with clause 8 as she had interpreted it.

D. Application of the *Isaacs* principle to the facts found by the judge

[84] Although the *Judgment* must be set aside, I would not remit this matter to the Court of King's Bench because the judge made all the findings of fact necessary to apply the *Isaacs* principle in resolution of this matter. In her *Judgment*, the judge found as a fact that:

(a) Mr. Bue had made an investment of $53,873 in a fictitious company called "Main Bit Ltd." based on an internet advertisement (at para 14);

(b) Mr. Bue sent over $190,000 CAD to the "Ministry of Justice at the United Kingdom" to obtain compensation for his investment in the fictitious company (at paras 15-16);

(c) Mr. Bue broke contact with the "Ministry of Justice at the United Kingdom" when they asked for another payment, in the amount of $75,000 USD (at paras 15-16);

(d) Mr. Bue received contact from "Funds Recall", which identified itself as a "Cybercrime agency", but he "does not appear to have given cash to 'Funds Recall'" (at para 17);

(e) Mr. Bue then agreed to send $80,000 to a third party posing as the "FBI", after he received an email from them sent from a Gmail account requesting his "participation in a 'dummy money transfer' to assist in dismantling the illegal operation" to which he had "fallen victim" and providing him with a cryptocurrency wallet for that purpose (at para 18);

(f) Mr. Bue provided the "FBI" with remote access to his computer and to his email accounts and gave the "FBI" unsupervised full control over them (at para 19);

(g) Mr. Bue did not inform HoneyBadger that he had been defrauded in the recent past (at para 21);

(h) Mr. Bue did not tell HoneyBadger that he was purchasing Bitcoin to give to the "FBI" or any third-party beneficiary (at para 21);

(i) Mr. Bue himself made several purchases of Bitcoin from HoneyBadger via email where he directed it to deposit the Bitcoin into the cryptocurrency wallet controlled by the third party posing as the "FBI" (at para 23);

(j) Mr. Bue did not specify a maximum withdrawal limit on the PAD agreement (at para 24); and

(k) Mr. Bue agreed to the terms of the Transaction Agreement as proposed by HoneyBadger, which allowed him and the "FBI" to purchase Bitcoin through

> HoneyBadger by way of instructions emailed from his personal email account (at para 26).

[85] The judge was, however, far more critical of Mr. Bue's conduct later in her reasons when reviewing the facts as she had found them, where she described findings that are directly relevant to the application of the *Isaacs* principle, as noted earlier:

> [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 Honey Badger 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. …
>
> (Emphasis added)

[86] Simply put, on the judge's findings of fact, Mr. Bue actively allowed a third party to defraud him and therefore, under the *Isaacs* principle, he must bear that loss.

V. DISPOSITION

[87] The appeal must be allowed, and the cross-appeal must be dismissed. HoneyBadger is entitled to the $200,000 held by the Court of King's Bench in the judicial centre of Swift Current.

[88] Accordingly, I would set aside the *Judgment* and direct the Local Registrar of the Court of King's Bench in Swift Current to release the funds held by that Court to HoneyBadger upon the expiration of the 60-day period in which Mr. Bue may appeal from this result to the Supreme Court of Canada, provided he has not by then filed an application for leave to appeal to that Court.

[89] I would award costs in the summary judgment application at the Court of King's Bench to HoneyBadger on Column II of that Court's tariff and one set of costs in the appeal and cross-appeal to HoneyBadger on Column 3 of the Tariff in this Court.

"Caldwell J.A."

Caldwell J.A.

I concur. "Kalmakoff J.A."

Kalmakoff J.A.

I concur. "Bardai J.A."

Bardai J.A.