The Honey Badger Should Care (About Loss Allocation Arising from BEC Fraud)

December 11, 2025

The murky waters of the new digital economy are fertile ground for financial criminals: a careless click on a phishing link, or a single call to a gullible recipient can allow the threat actor to reel in the "catch of the day", leaving numerous victims in their wake.

Where the threat actor gains access to the victim's email account and initiates payment to a vendor, who bears the loss between innocent parties? A case from the Saskatchewan Court of King's Bench is the latest addition to the body of Canadian law mapping out some answers to that vexing question.

Honeybadger Enterprises Ltd. v. Bue, 2025 SKKB 123 is a timely reminder to businesses and consumers alike – particularly those involved in selling or purchasing cryptocurrency – of the importance of clear contractual terms allocating loss for payment instructions made by email, and the importance of strict adherence to contractual instruction verification protocols.

The *Honeybadger* case contains useful analysis on the enforceability of contractual terms for loss allocation arising from digital payment instructions, the role of the doctrine of mistake of fact in loss allocation, and the availability of apportionment as between innocent parties following a fraud loss.

Key Takeaways

1. While contractual terms allocating loss to the payor or purchaser can be helpful to the payee or vendor, in order to rely on the contractual allocation, the beneficiary of such a provision must strictly adhere to any instruction verification protocols stipulated in the contract. If the contract stipulates a specific method to verify payment instructions, the payee or vendor must follow those requirements. A failure to comply can be a cause of the fraud loss, and may shift liability, or apportion liability, back to the payee or vendor.
2. Vendors should review their pre-authorized debt agreements and protocols for processing payment instructions those agreements. In particular, where the PAD agreement stipulates a method to verify payment instructions – by password, security code or signature – the payee must strictly follow the stipulated protocol.

3. The doctrine of mistake of fact may be available to allocate liability where one of the innocent parties was in a position to avoid the loss, and the other party detrimentally changed position in good faith. The *Honeybadger* case leaves open the possibility that failure to comply with regulatory obligations, such as anti-money laundering or FINTRAC compliance, could be capable of vitiating the good faith requirement under the doctrine.
4. Apportionment of the fraud loss as between payor and payee may be available where both parties were contributorily negligent, or where a failure to comply with the terms of the contract contributed to the loss.

Background

Honeybadger Enterprises Ltd. operates an over-the-counter cryptocurrency business and processes purchases made by its clients through PAD Agreements. The PAD agreements allow Honeybadger to withdraw funds directly from a customer's bank account upon receipt of payment instructions.

One of Honeybadger's clients, Mr. Bue, entered into a PAD Agreement in which Honeybadger was authorized to purchase cryptocurrency for Mr. Bue, draw funds from Mr. Bue's account, and then deposit the cryptocurrency into Mr. Bue's digital asset wallet.

Mr. Bue had been socially engineered by a threat actor impersonating an FBI agent. The threat actor led Mr. Bue to believe he had been recruited to participate in dismantling an illegal operation, and that he needed to deposit Bitcoin to a digital wallet address in connection with that operation. The threat actor provided the wallet address to Mr. Bue.

In connection with the social engineering scam, Mr. Bue provided remote access to his computer to the threat actor. Thereafter, Mr. Bue did not realize that the threat actor gained access to, and had control of, his email account.

Mr. Bue provided legitimate instructions to Honeybadger by email to purchase $40,000 of Bitcoin, to be deposited to the wallet address provided by the threat actor. Honeybadger processed those payments pursuant to the PAD agreement, and deposited the cryptocurrency into the wallet, as instructed.

Unbeknownst to Honeybadger and Mr. Bue, the threat actor then sent additional emails to Honeybadger providing instructions to purchase $200,000 of Bitcoin. Honeybadger processed those payments pursuant to the PAD agreement and deposited the cryptocurrency into the digital wallet.

Mr. Bue later discovered the fraud, including the payment instructions provided by the threat actor from his email address. Mr. Bue then asked his credit union to cancel the payments totalling $240,000, which it did. Honeybadger sued Mr. Bue for the amount of the Bitcoin deposited to the wallet.

The Court's analysis and decision

The Court held that Mr. Bue was liable for the $40,000 in payments that he initiated, and that Honeybadger and Mr. Bue equally contributed to the loss for the $200,000 in

payments initiated by the threat actor. As a result, Mr. Bue was ordered to pay to Honeybadger $140,000.

The PAD agreement contained the following term regarding verification of payment instructions:

> 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.

The Court found that Honeybadger did not follow the "password or security code or other signature equivalent" verification requirement with respect to any of the transactions. The Court rejected Honeybadger's argument that an email from Mr. Bue was a "signature equivalent" under the provision.

The Court cited, with approval, *Du v. Jameson Bank*, 2017 ONSC 2422 for the following propositions:

1. A financial institution has a common law and contractual obligation to honour its customers' instructions, and where a customer provides a payment instruction, a financial institution is entitled to treat the mandate at face value.
2. If the terms of contract do not require the financial institution to question or inquire about the accountholder's payment instruction, then no further inquiry is required by to process the payment.
3. Where the terms of account agreement permit the accountholder to provide payment instructions by email, and where the financial institution is contractually entitled to follow those instructions, the accountholder will bear the loss for instructions provided by a threat actor where the email account had been compromised, so long as the financial institution had no reason to doubt the authenticity of the instruction.
4. The Court will give effect to exclusions of liability contained in account agreements.

However, unlike in *Jameson Bank*, the contractual terms between Honeybadger and Mr. Bue did not stipulate that Honeybadger could rely solely on email instructions from Mr. Bue. Rather, the terms of the PAD agreement required an additional step to perfect instructions: issuance, and corresponding verification, of a password, security code or signature equivalent. As such, Honeybadger could not rely on the payment authorization provision in the agreement to hold Mr. Bue liable for the instructions.

The Court considered the doctrine of mistake of fact to allocate loss for the payment instructions. The doctrine may be available as between two innocent parties and provides that: (a) the party who was in a position to prevent the loss should bear it; and (b) a person who receives money obtained by fraud in satisfaction of a *bona fide* debt, without notice of the fraud is entitled to retain the money. However, the change of position must be in good faith.

In this case, the Court found that Mr. Bue's naivete and ignorance was at the heart of the fraud. Had he made any mention to Honeybadger of the "FBI" scam, Honeybadger would not have processed the payments, and the fraud would have been discovered. But for Mr. Bue's carelessness in allowing the threat actor to gain remote access to his computer, Honeybadger would not have drawn on the PAD or deposited the Bitcoin into the wallet.

Mr. Bue argued that Honeybadger failed to comply with its obligations as a Money Services Business as prescribed by FINTRAC, it could have prevented the loss had it done so, and Honeybadger's change of position was not in good faith as a result. Honeybadger argued that it complied with its FINTRAC obligations. However, the parties did not file expert evidence on the standard of compliance, so the Court was unable find that Honeybadger failed to comply with FINTRAC requirements.

However, the Court found that Honeybadger failed to comply with the instruction verification processes stipulated by the PAD agreement by failing to "issue" a password, security code or signature equivalent, instead relying only on email communication. Had Honeybadger followed the PAD agreement, the fraud loss would have been avoided.

While Mr. Bue's conduct put the fraud in motion, Honeybadger's non-compliance with its agreement failed to prevent the fraud loss. The Court held that both parties must equally share liability for the payment instructions provided by the threat actor.

By

Hunter Parsons, Sadie Howe, Olivia Ramos

Expertise

Disputes, Cybersecurity, Privacy & Data Protection, Banking & Financial Services, Financial Services

---

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749