Banks may be liable for negligent transfer of hacked accounts

This column was originally published in The Journal Record on March 9, 2020.

When asked by a reporter why he robs banks, notorious criminal "Slick Willie" Sutton replied, "Because that's where the money is." While banks still have the money, the nature of the crime has evolved with technology. Today's modern bank robber is often armed with nothing more than a mouse and keyboard, and the preferred tools and techniques of their trade are phishing and malware.

Hackers infiltrate businesses and individuals alike, typically using "social engineering" tactics to gain trust and access to an employee's email account, to cite a common example, and re-route money from the rightful owner's bank account to their own. While there are stiff penalties for a criminal caught in the act, it may come as a surprise that a bank that authorizes a wire transfer to a hacker's account could be liable to the rightful owner.

Article 4A of the Uniform Commercial Code was enacted in response to the growth of electronic funds transfers and the crime that evolved in its wake. Under Article 4A, a bank is liable to a customer for the full amount of a negligently processed wire received by a hacker, including interest.

In the most basic terms, a bank is liable to its customer for a negligent wire transfer when (1) the customer did not authorize the transfer and (2) the transfer cannot be enforced against the customer because either (a) the transfer was not

authorized by an employee of the customer or (b) a third party (outside hacker) initiated the transfer. At first glance, this may seem to be a slam-dunk trigger for liability to an aggrieved customer. But banks can take proper steps to insulate themselves from any liability under Article 4A.

To avoid liability, the bank must first prove three things: First, that it and the customer had an "agreed security procedure," which are steps put in place, to which both the bank and customer agree by contract, to verify that a payment order or communication is between the bank and the customer. This is most commonly accomplished in the customer and bank's initial account agreement.

Second, the bank must prove that it complied with the agreed security procedure and that such procedure is "commercially reasonable." In other words, the procedures are to be in line with that which someone familiar with the industry would regard as sufficient and realistic. Examples of what constitutes "commercially reasonable" are explored below.

Finally, the bank must prove that it not only followed the security procedure, but that it initiated the wire transfer in "good faith." In other words, the bank must prove that it acted with honesty in fact and observance of reasonable commercial standards of fair dealing.

So how does a bank best avoid liability?

In practice, cases under Article 4A often hinge on whether the bank's security procedure is commercially reasonable. In order to meet this threshold, a bank is expected to have better than single-factor identification. The wire transfer should require the customer to input at least two of the following: (1) something the customer knows, such as a password; (2) something the customer has, such as an IP address; or (3) something the customer is, such as a fingerprint or voice scan.

With cybercrime on the rise, it is crucial for any bank to both protect its customers and insulate itself from potential liability. Requiring multi-factor identification is no guarantee for a bank to avoid liability under Section 4A, but it is one relatively easy way for a bank to better protect itself and its customers.