Bulletin | Cybersecurity, Privacy and Data Protection

March 2020

Managing the risks of email compromise fraud

Email compromise fraud is an increasingly common cyber risk that can result in significant losses and liabilities to targeted organizations and their customers and business partners. Three Canadian courts have considered claims resulting from email compromise fraud. The decisions illustrate the risks associated with email compromise fraud, and provide guidance for managing those risks.

Email compromise fraud

Email compromise fraud, also known as Business Email Compromise (BEC) or Email Account Compromise (EAC) fraud, is a sophisticated scheme that targets businesses and individuals who perform electronic funds transfers. The scheme commonly involves emails sent from hacked or spoofed internal (e.g. senior officer) or external (e.g. vendor or customer) email accounts that give fraudulent instructions to make electronic payments to the account of the fraudster instead of the account of the intended payment recipient. Email compromise fraud often involves the use of sophisticated social engineering to make fraudulent emails appear authentic.

According to the U.S. Federal Bureau of Investigation's *2019 Internet Crime Report*, email compromise crimes accounted for almost half of the losses – an estimated $1.77 billion – from all internet and cybercrimes reported to the F.B.I. in 2019. According to the Canadian Anti-Fraud Centre website, email compromise fraud is the second highest for monetary loss out of over 40 types of reported fraud.

Liability for losses resulting from email compromise fraud

Email compromise fraud can result in disputes over which of the affected parties must bear the financial loss – the organization whose email account was compromised or the organization deceived into making a misdirected payment. This issue has been considered in three reported decisions by Canadian courts.

Fraudulent emails from bank customer

Du v. Jameson Bank involved a dispute between a bank and its customer over liability for unauthorized transfers totaling USD $135,000 from the customer's bank account, which were made by the bank based on instructions in fraudulent emails sent from the customer's email account by an unknown fraudster who allegedly hacked into the account. The emails included details (e.g. the name of the customer's financial advisor and his bank account at another bank) that made the emails appear to be authentic. The funds were not recovered.

The customer sued the bank to recover the misappropriated funds, and the bank relied on protective provisions in the agreement that governed the customer's account. The agreement permitted the customer to give electronic instructions to the bank through a specified email address, and permitted the bank to rely on email instructions that appeared to be from the customer and which the bank believed in good faith to be genuine. The agreement provided that the bank was not liable for any damages or losses resulting from a funds transfer unless the bank was grossly negligent or engaged in willful misconduct. The agreement provided that the customer was responsible for the accuracy of all transfer instructions, and required the customer to use security systems to prevent and detect fraudulent and unauthorized instructions.

The Ontario Superior Court of Justice held that the customer was bound by the account agreement regardless of whether he read it. The court found that the bank was not negligent, and did not act improperly, by accepting the fraudulent email instructions because the bank had no reason to doubt the authenticity of the instructions. The court held that the bank was not obligated to question the instructions. The court reasoned that the fact that a bank customer is a victim of fraud does not result in an automatic transfer of liability to the bank. The court concluded that it was the customer's failure to secure his email account that led to the fraudulent transfer instructions, and that the account agreement was a complete defence to the customer's claim against the bank. The court dismissed the lawsuit.

Fraudulent emails from adverse party's lawyers

St. Lawrence Testing & Inspection Co. Ltd. v. Lanark Leeds Distribution Ltd. involved a dispute over a misdirected $7,000 settlement payment made based on fraudulent email instructions. The settlement agreement required the defendant to pay the settlement amount to the plaintiff's lawyers' trust account at a specified bank. Before the defendant paid the settlement payment, a cybercriminal hacked the email account of a paralegal employed by the plaintiff's lawyers, and sent the defendant fraudulent emails with instructions to make the payment to a different bank account in the name of an individual (rather than the plaintiff's lawyers). The defendant paid the settlement amount to the criminal's account in accordance with the fraudulent instructions. The funds were not recovered.

The plaintiff applied to court for an order that the defendant pay the settlement amount to the plaintiff. The defendant resisted the order on the basis that it had already made the required payment in accordance with instructions from the plaintiff's lawyers. The defendant relied on the decision in *Du v. Jameson Bank*, and argued that the plaintiff should bear the loss resulting from the cybercrime.

The Ontario Small Claims Court held that where a cybercriminal takes control of the email account of "Victim A" and, impersonating Victim A, sends instructions to "Victim B" to transfer funds intended for Victim A (or a third party) to the criminal's account, Victim A is not liable for the loss unless: (1) Victim A and Victim B are parties to a contract that authorizes Victim B to rely on email instructions from Victim A and, assuming compliance with the contract, shifts liability for loss resulting from fraudulent payment instructions to Victim A (as in *Du v. Jameson Bank*); (2) there is evidence of willful misconduct or dishonesty by Victim A; or (3) there is negligence on the part of Victim A. The court held that there was no evidence that the hacking of the paralegal's email account was the result of any negligence on the part of the plaintiff's lawyers or the paralegal. The court concluded that the defendant had to bear the loss resulting from the fraudulent emails, and the plaintiff was entitled to a judgment requiring the defendant to pay the settlement amount to the plaintiff.

Fraudulent emails from supplier

Opus Consulting Group Ltd. v. Ardenton Capital Corporation involved a dispute over a fraudulently misdirected payment of invoices for computer hardware. The plaintiff supplier issued two invoices totaling $186,000 to the defendant customer. The customer requested electronic payment instructions, and the supplier's employee sent an email with instructions. Less than an hour later, the customer received a second email, purporting to be from the same individual who sent the original payment instructions email, with changed instructions to make the payment to a different account at a different bank to the credit of a different company. The customer made the payment in accordance with the changed payment instructions. The supplier subsequently notified the customer that the payment had not been received, and the parties discovered that they had been victims of an email compromise fraud and that the customer had paid the funds to a bank account controlled by an unidentified cybercriminal. The funds were not recovered.

The supplier demanded the customer pay the invoices. The customer refused on the basis that it was entitled to rely on the payment instructions email sent from the supplier's email account, and alleged that the supplier was responsible for its email system security breach. The supplier sued the customer and obtained a pre-judgment order requiring the customer to pay funds into court. The customer applied to set aside the payment order.

The British Columbia Supreme Court set aside the payment order for technical non-compliance, and further held that the order should not have been issued because there were serious issues to be tried as to whether the supplier was responsible for not protecting its email system and other failings that allowed the cybercriminal to send the fraudulent payment instructions email, and whether the customer was responsible for complying with the fraudulent payment instructions. The court directed those issues be determined at trial.

The decision in *Opus Consulting Group v. Ardenton Capital Corporation* is consistent with the decision of the U.S. Court of Appeals in *Beau Townsend Ford Lincoln v. Don Hinds Ford*, in which the court held that a trial was necessary to determine which party "was in the best position to prevent the fraud".

Comment

The decisions in *Du v. Jameson Bank*, *St. Lawrence Testing & Inspection v. Lanark Leeds Distribution*, and *Opus Consulting Group v. Ardenton Capital Corporation* illustrate how the allocation of responsibility for losses resulting from an email compromise fraud will depend on the particular circumstances, and that a costly and time-consuming trial might be necessary if the relevant facts (including the parties' relative culpability) are in dispute.

The decisions also illustrate the potential importance of a well-drafted agreement that expressly addresses the use of email for payment-related communications and allocates responsibility for losses and liabilities resulting from email compromises and similar circumstances.

The Canadian Anti-Fraud Centre, the Canadian Centre for Cyber Security, the Competition Bureau of Canada and the F.B.I. have published guidance for proactive measures to help organizations avoid being victimized by email compromise fraud. The guidance emphasizes the importance of people (e.g. education and training), processes (e.g. internal payment approval procedures, and in-person/telephone verifications of email instructions) and technologies (e.g. robust email password policies and email security technologies).

Insurance can be an effective way to manage the residual risk of email compromise fraud. However, traditional crime insurance coverage for "computer fraud" or "funds transfer fraud" might not apply to losses or liabilities resulting from funds transfers caused by email compromise fraud. It might be necessary to obtain insurance for "social engineering fraud" in addition to traditional crime insurance. Organizations seeking to obtain insurance for email compromise fraud should obtain appropriate advice from legal counsel and an experienced insurance consultant when purchasing cyber insurance or when determining whether an existing insurance policy provides sufficient coverage. For more information, see BLG bulletin *Insurance for Cybersecurity Incidents and Privacy Breaches*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com