Dealing with Phishing Post Loss

The aftermath of a successful wire fraud phishing expedition is stressful and unpleasant for all parties involved. After all, it can be quite difficult to acknowledge and take ownership of a substantial loss to your client due to a costly, albeit inadvertent, oversight. As a result, the parties involved are left to determine who bears the burden of liability when the dust settles. When payment orders or funds transfer requests are provided to the bank or financial institution, the sender quite often believes that it is the responsibility of the bank or financial institution to exercise caution and prudence in disbursing the funds if the transaction appears "suspicious" or does not quite make sense. Conversely, however, the banks or financial institutions believe it is the sender's responsibility to take precautionary measures to avoid, as much as reasonably possible, becoming the victim of a wire fraud incident. This raises the question, then – what do the courts have to say about which party is liable in this instance?

Case law and codified statutes suggest that the risk of loss often falls on the sender if the bank has complied with commercially reasonable security procedures and has accepted the payment order in good faith. Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank and the circumstances of the customer known to the bank – such as the size, type, and frequency of payment orders normally issued by the customer to the bank. Cal. Com. Code § 11202(c). The relevant authority can be found in Article 4A of the Uniform Commercial Code ("UCC"), which is codified in division 11 of the California Commercial Code. Like California, all 49 other states have codified Article 4A, which "provides a comprehensive body of law to govern the rights and obligations resulting from wire transfers." Due to the great risks associated with the large amounts of money that are typically transferred by banks on a daily basis, the Article 4A provisions were much needed in allocating the risk of loss appropriately in light of the ever-growing wire fraud and cyber-crime statistics.

The provisions in the California Commercial Code are pervasive in this field and are designed to protect the banks from being sued by the sender of funds based on common law claims, such as negligence, that would be inconsistent with these provisions. Per the Supreme Court of California's ruling in *Zengen, Inc. v. Comerica Bank* (2007) 41 Cal4th 239, common law claims are displaced by provisions of division 11 where (1) the common law claims would create rights, duties, or liabilities inconsistent with division 11; and (2) where the circumstances giving rise to the common law claims are specifically covered by the provisions of division 11.

What this means is that the courts in California will use the provisions set forth in division 11 of the California Commercial Code to allocate liability among the parties when the issue at-hand is specifically covered by said provisions relative to the transfer of funds. For instance, if sender sends an authorized payment order to the bank and the bank follows its commercially reasonable security procedures and accepts the payment order in good faith, it is very unlikely that the sender would prevail if it sued the bank for negligence in disbursing the funds pursuant to the payment order. It is therefore crucial, for both senders and banks to understand the duties and liabilities imposed upon them in order to be efficient in minimizing the risks associated with wire transactions.

Division 11 of the California Commercial Code specifically addresses this issue in providing a framework for the duties imposed on each party. Section 11202(a) states that if the payment order is signed by someone with authority to act on behalf of the company, then it is an authorized order.

The key, then, is for the sender to ensure that their authorized order contains accurate information (i.e. the actual seller's wire instructions in a real estate transaction as opposed to a fraudulent perpetrator's wire instructions). Per section 11203 of the Commercial Code, the burden on sender is to "supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached."

Under section 11203(a)(2) of the Commercial Code, the sender may avoid the loss resulting from such a payment order if the sender can prove that the fraud was **not** caused, directly or indirectly, by a person who was "(i) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or (ii) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault. Information includes any access device, computer software, or the like." [Emphasis Added]

In essence, if a cyber-criminal successfully intercepts email communications within a company to provide fraudulent wire instructions for the disbursement of funds, and the company sends a payment order to the bank pursuant to these wire instructions, the company will bear the burden of liability if the bank accepts the payment order in good faith and the transaction does not raise any red flags relative to the company's usual banking patterns or activities (if the company has elected to have these security procedures in place).

Case law and division 11 further suggest that even if the payment order is sent by a perpetrator posing as an authorized sender, the burden of liability still falls on the sender if the perpetrator has breached the sender's security protocols so as to facially submit the payment order as the sender. In August of 2001, the agencies of the Federal Financial Institutions Examination Council ("FFIEC") issued guidance titled "Authentication in an Internet Banking Environment," which requires banks and financial institutions to use authentication procedures such as PINs, security questions, fingerprints, etc., to authenticate their customers' identity in transactions. If banks are in compliance with the FFIEC guidelines, it is therefore crucial to make it very difficult, if not impossible, for cyber-criminals to breach these commercially reasonable security procedures on the banking customer's end.

"Breach of a commercially reasonable security procedure requires that the person committing the fraud have knowledge of how the procedure works and knowledge of codes, identifying devices, and the like. That person may also need access to transmitting facilities through an access device or other software in order to breach the security procedure. This confidential information must be obtained either from a source controlled by the customer or from a source controlled by the receiving bank. If the customer can prove that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer or from a source controlled by the customer, the loss is shifted to the bank." Cal Com. Code § 11203 Uniform Commercial Code Comment.

With the foregoing in mind, it is important for banks to employ reasonable security measures and to offer said security procedures to their customers. The banks should be diligent in complying with these security procedures and any agreement in place with the customer in order to avoid liability.

On the other hand, it is important for real estate companies to agree to utilize as many security procedures offered by the bank as reasonably possible. A sender that has refused to employ the security procedures offered by its bank cannot shift the burden of liability to the bank should it suffer a loss as a result of a wire fraud that could have been prevented with these precautionary measures. In addition, real estate companies should establish internal security procedures such as dual authentication systems for customer security, proper personnel training, data encryption and secure emails, malware and virus detection and protection software, etc. Dual customer authorizations should entail two different access devices, such as authentication by email and by phone, using a primary phone number that was initially on file. Real estate personnel should be wary of any variance in communications via email, such as receiving correspondence from different (but very similar) email addresses purporting to be an authorized party in the transaction, grammatical or stylistic errors or changes, last-minute changes to wiring instructions, etc. Real estate companies must take these cyber-hacking wire fraud risks seriously as grave consequences are in store in the event of a successful fraudulent transaction.

In the unfortunate even that such a transaction has been completed and the funds have been disbursed to a fraudulent party, the real estate company must act quickly in notifying the bank of the fraudulent transaction in an attempt to recover the funds. The sooner the bank or financial institution is notified, the more likely it will result in mitigation of loss, if possible. Proper officials, such as local law enforcement and the Federal Bureau of Investigation ("FBI"), should also be notified as soon as possible. An IC3 internet crime complaint should be filed with the FBI online via the following link: https://www.ic3.gov/complaint/default.aspx.

As the real estate and finance industries increasingly rely on technological tools and internet-based systems to facilitate escrow transactions, the cyber-criminals, too, are formulating clever tactics to keep up with these advancements in order to capitalize on any "areas of weakness" in these systems. As a result, all parties involved in these transactions need to be very prudent in safeguarding their information in order to prevent these attacks as much as possible.

This article was written by Jennifer Felten, Esq. Her law firm, RELAW, APC, provides legal representation and counsel on various forms of real estate transaction and litigation issues for individuals, real estate professionals and escrow companies. She can be reached by phone at (805) 265-1031 or via email at jennifer@relawapc.com. The firm's website is located at www.relawapc.com.