An Escrow Owner's Fight Against Cyber Fraud and Her Unrelenting Efforts to Stay In Business

By Julie Bonnel-Rogers, Esq.
Silicon Valley Law Group

California Escrow Association, you have a hero among you and her name is Michelle Marsico. Michelle Marsico is the owner and founder of Village View Escrow, Inc. in Redondo Beach, California. In 2008 Michelle opened Village View Escrow with two employees. As a licensed escrow agent governed by the State of California's Department of Corporations, Michelle Marsico's most basic task was to safeguard her clients' funds. As such, choosing a reliable and reputable financial institution with which to bank was of utmost importance. After meeting with account managers from a local bank and getting what she described as a safe "feeling," Michelle Marsico and Village View Escrow began a business banking relationship with Professional Business Bank in July 2008.

Cyber Fraud Took Nearly a Half a Million Dollars from Village View Escrow's Bank Account

On March 16-17, 2010 Village View Escrow's account at Professional Business Bank was hacked by unknown outsiders who, through 26 consecutive payment orders which were alarmingly suspicious, ultimately stole $465,555.97 from Village View Escrow's account. What followed for the next two and half years was Michelle Marsico's battle against cyber fraud and her unrelenting efforts to stay in business.

Cyber fraud has been described by some experts in the security field as a national crisis. Escrow companies are among the most heavily targeted business sectors for cyber fraud because of their large money deposits. There are various methods in which cyber thieves can gain access to online business accounts. One of the most common ways to breach security is through ***phishing***. Phishing is an outside attempt to acquire private information such as usernames, passwords or credit card details by masquerading as a trustworthy or familiar entity. For example, a phishing decoy might involve a faux e-mail message from Facebook or Federal Express which requests information which appears reasonable. By opening the e-mail, and/or responding to the same, a user may be providing access to an online account through sophisticated mechanisms.

The Fallout After the Cyber Fraud

Shortly after the wire transfer fraud, Village View Escrow was subjected to investigation from local and national law enforcement that needed to rule out foul play. Michelle Marsico had to answer to police agents, her customers and clients, her employees and vendors about the loss of nearly a half million dollars.

Further, in accordance with state regulations, Village View Escrow was required to self-report the loss of customer funds to the Department of Corporations ("DOC"). Thereafter the DOC conducted an audit of Village View Escrow's business at a direct cost to Village View Escrow. Village View Escrow's professional license was put in jeopardy. In order to survive, Village View Escrow hired legal counsel and a certified public accountant to represent it to the DOC and took out interest bearing loans to balance its books. Thanks to the work of qualified professionals, Village View Escrow's doors remained open.

Justifiably, customers and clients of Village View Escrow grew concerned about the lost funds. Some threatened legal action. Others grew impatient as Village View proceeded through its DOC audit. The threat of bankruptcy loomed.

Meanwhile, Michelle Marsico, her IT representative Mr. Ken Hollomon of HCS Development Group, Inc. and family began an underground campaign to track down the stolen funds which were wired to "mules" for forwarding out of the country. ***"Mules"*** are intermediaries in the continental United States arranged by the cyber thieves to receive small bundles of payment. The cyber theft must be accomplished in small amounts to avoid Patriot Act and Bank Secrecy Act detection, and cyber thieves are sophisticated enough to know how to solicit unsuspecting accomplices via Craigslist and other online sites to receive the stolen money, keep a small payment and forward the money out of the country via Western Union. Michelle Marsico and her team tracked down contact information for the mules who through diligent sleuthing on Facebook and Google. Thereafter, they called the mules and sent e-mails threatening legal action and demanding the return of the stolen money. Some mules refused to cooperate. Others, however, were unsuspecting pawns who cooperated and returned the money. $72,000 was recovered in total. However, Village View Escrow was still missing $393,000.

Continued on page 16

Wire Transfer Fraud Law

Article 4A of the Uniform Commercial Code (which has been adopted by the majority of the states including California by way of Division 11 of the California Commercial Code) applies to "funds transfers." Simply stated, "funds transfers" are instructions to a bank to pay out money to a specified beneficiary. Significantly, Division 11 of the California Commercial Code sets forth the ***exclusive*** rights and remedies of parties with respect to wire transfer fraud ("WTF"). In *Zengen, Inc. v. Comerica Bank* (2007) 41 Cal.4th 239 the California Supreme Court confirmed that liability for damages resulting from a bank's release of unauthorized payments must be exclusively analyzed and limited under the California Commercial Code. This means that common law claims such as negligence, breach of contract and fraud, and the damages that attach to them, are generally precluded from being asserted by a victim of wire transfer fraud. This, in turn, severely limits the avenues of recovery by victims of wire transfer fraud, and makes it difficult for a victim of cyber fraud to recover against a bank. It also makes wire transfer fraud cases unappealing to lawyers.

In California, victims of WTF typically will assert a claim against its bank for the recovery of its lost funds under California Commercial Code section 11102 which addresses the risk of loss between a customer and its bank for fraudulent wire transfers. Section 11102 sets forth a two prong analysis for liability: (1) whether the security procedure employed by the bank was "commercially reasonable"; and (2) whether the bank accepted the payment order in "good faith." These two factors are the subject of a newly emerging area of law being litigated across the country through corresponding state codes, sometimes with inconsistent results.

The Cost of Filing a Wire Transfer Fraud Lawsuit Against a Bank

The law, as set forth above, presents a business owner who falls victim to wire transfer fraud, like Village View Escrow, in a precarious position. The business owner places her money with a bank for safe keeping and distribution. Cyber thieves breach the security and gain online access to the account from which they steal several bundles of money. As a result, the business owner can lose hundreds of thousands of dollars in a matter of minutes. In these types of scenarios, the bank typically denies liability. The business owner must then expend ***further*** money it does not have to recover a limited and defined set of damages set forth under Division 11 of the Commercial Code which limits damages resulting from wire transfer fraud to the actual amount of money stolen plus interest-***nothing more***. Consequential damages such as audit fees, interest on loans, costs and attorney fees are not recoverable.

Further, most banks are in a financial position to defend themselves against legal claims as to whether their security procedure was "commercially reasonable" and/or whether the bank accepted the payment order in "good faith." Banks can afford security experts and computer experts to bolster their defense. It behooves the banks to do so in order to protect the existing legal structure which was arguably written to the advantage of financial institutions in the first place. Conversely, due to the cyber theft and other financial restrictions, a small business such as Village View Escrow is in no financial position to litigate, with little incentive by way of damage recovery to do so under the current existing legal structure.

Michelle Marsico persuaded a childhood friend who happened to be an attorney with a sympathetic heart to take her case. Mr. Kim Dincel of Silicon Valley Law Group agreed to represent Village View Escrow in a claim against Professional Business Bank just a few short weeks before the one year statute of limitations ran.

Michelle Marsico was a soldier in the legal trenches by providing her attorneys with information and personal commitment every step of the way. She was present at each juncture of the lawsuit. She attended numerous hearings and depositions. She hosted her legal team in her own home when they arrived from Northern California to attend legal proceedings because there

Continued on page 17

BE PROACTIVE!

Ten Cyber Security Questions to Ask Your Financial Institution BEFORE You Sign an Online Banking Contract

Escrow companies are targeted by banks for the same reason they are targeted by cyber thieves: they make large deposits. Large deposits help to capitalize a bank, which makes a bank more profitable. Representatives of banks may approach escrow companies and provide escrow company owners with specifically tailored banking presentations and promises of safety, services and escrow-specific business amenities. An escrow company must carefully place its trust in, and rely on, the bank to protect its funds. Banks want the escrow companies as customers, so choose cautiously. The right bank can be your best ally in the battle against cyber fraud.

Here is a list of questions you should discuss with your financial institution before you grace them with your patronage:

QUESTION 1: Do you abide by FDIC and FFIEC Guidelines for wire transfer transactions?

The FDIC (Federal Deposit Insurance Corporation) and FFIEC (Federal Financial Institutions Examination Council) monitor financial institutions. The FDIC and the FFIEC have issued guidelines and advisories for wire transfer security. The guidelines are issued industry-wide, but financial institutions are not obligated under the law to adopt the recommendations. Seek out a bank that integrates the FDIC and FFIEC's guidelines into their banking practices.

QUESTION 2: Does the financial institution work with a security provider (sometimes referred to as a "core processor")?

Not all banks are equal and not all security providers are equal. Banks that work with security providers and opt for "premium" or high level security packages generally are provided with more security against of cyber fraud than others. Choose a bank with a reputable security provider and a high level security provider package.

QUESTION 3: Does the financial institution have a fraud protection department or representative?

Cyber fraud is evolving so the bank must be vigilant in its efforts to stay updated and proactive in its fight against cyber fraud. The best banks are the ones who are proactive. This means that

the bank has a department or at least employee assigned to obtaining current information about cyber security.

QUESTION 4: Does the financial institution *multifactor* authentication for security?

There are three categories of security authentication a bank may offer its customer in order to guard against fraud:

- Something the user knows (e.g., password, PIN);
- Something the user has (e.g., ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint)

The best security is "multifactor" which means that it is comprised of at least two different categories of security as set forth above. The two levels should be from different categories-not the same (layered single factor authentication is not as prohibitive).

QUESTION 5: Does the financial institution offer tokens as a security option?

Tokens require the escrow owner to verify a payment order by communicating a password conveyed through the token. Tokens can afford the business owner with an extra layer of security and an added level of involvement in the protection of its funds.

QUESTION 6: Does the financial institution offer "call backs" as a security option?

Call backs require the bank to contact the escrow owner to verify a payment order by telephone. Like tokens, call backs can afford the business owner with an extra layer of security and an added level of involvement in the protection of its funds.

QUESTION 7: Does the financial institution have cyber fraud insurance?

In the ever-evolving world of cyber fraud, an escrow company can never take too many precautions in protecting its client's funds. Insurance is an excellent safety net in this regard.

QUESTION 8: Does the financial institution have a recovery protocol for the recovery of funds stolen through cyber fraud?

Time is money in the aftermath of cyber theft. If the financial institution has a satisfactory recovery protocol, it will have an immediate plan to implement upon a report of cyber theft. The recovery efforts should extend beyond the average 9 am to 5 pm bankers' hours. It should involve pre established cooperative efforts amongst the financial institutions involved as well as efforts to directly pursue the recovery of funds from the "mules" paid to ferry the stolen funds out of the country.

QUESTION 9: If a business does fall victim to cyber theft, does the financial institution offer bridge loans to help your business survive in the aftermath of the cyber attack?

Sometimes when unfortunate events occur, a bank may offer a "bridge loan" to its valued customers. A bridge loan is an unsecured loan at a low interest rate to aid a customer in a time of need. Escrow companies should be considered valued bank customers because of the advantages the banks derive from the escrow company's large deposits. In the aftermath of a cyber attack, a bridge loan might make the difference between your businesses survival and its demise.

QUESTION 10: Does the financial institution have any suggestions about what a business can do to guard against a cyber attack?

A bank that is prepared for cyber fraud will have information about how a business can help protect its online accounts. Common suggestions include:

- Maintain a separate designated work station/ computer for online banking
- Limit access to social media sites by employees working on the designated work station/computer for online banking
- Train company employees to be vigilant for phishing attacks and to conduct online banking in a safe manner
- Check the company's account for wire transfer activity daily
- Report any and all suspicious activity to the bank immediately
- Keep the lines of communication open with the bank; know your banker's names and contact numbers
- Consider purchasing wire transfer fraud insurance through a general business policy
- Read and respond to correspondence from your bank regarding security updates and options. If you do not receive such correspondence, contact the bank for current information.

were no available funds for hotels. She continued to operate Village View Escrow to stay in business and to generate much needed funding for the lawsuit.

When a business owner like Michelle Marsico *does* choose legal action, creative pleading and diligent litigation can sometimes result in a favorable outcome for the business owner. That is what occurred in the case of Village View Escrow. In an unprecedented settlement which occurred the last business day before trial was to begin, Professional Business Bank agreed to pay Village View Escrow $600,000 – more than is authorized under Division 11 of the California Commercial Code.

Pay outs from banks to victims of wire transfer fraud do occur. Settlements and judgments are being reported across the country. Still, there are no guarantees when the business owner files suit. As the law stands right now, it is the business owners who usually bear the brunt of cyber theft by way of bankruptcy or legal expenses or pure, unrecoverable monetary loss. Occasionally, hardworking teams of professionals make a commitment to fight the system. Village View Escrow surrounded itself with such professionals and is an example of how a small business can stay in operation and successfully fight a formidable opponent.

Fear Not

There are mechanisms to guard against cyber theft. Security provider, bank and customer must be vigilant in setting up security procedures to detect, and advise of, suspicious activity. Ongoing and timely communication between security provider, bank and customer, can both curb the onset of cyber theft as well as assist in the recovery of lost funds in the aftermath of cyber theft. Also, insurance companies offer products to insure against the harsh realities of wire transfer fraud for proactive business owners.

Julie Bonnel-Rogers is an attorney at Silicon Valley Law Group in San Jose, California. She specializes in business litigation and is part of a grass-roots community of cyber fraud activists. For more information see *svlg.com* or contact Ms. Rogers directly at *jbr@svlg.com.*