# TABLE OF CONTENTS

EXECUTIVE SUMMARY ...................................................................................................................................................... 3
THE CYBERCRIMINAL: TOOLS AND TACTICS.............................................................................................................. 3
FIGHTING WIRE FRAUD: THE FINANCIAL INSTITUTION'S PERSPECTIVE ................................................................. 4
LEGAL LANDSCAPE ............................................................................................................................................................ 5
SHORING UP THE DEFENSES ........................................................................................................................................ 6
CONCLUSION ......................................................................................................................................................................... 7
Mention wire fraud in a room full of bankers, and you are sure to get a reaction. The transaction may take place within minutes, but the effects of wire fraud can last for months, sometimes years, in the form of protracted and costly litigation.

When wire fraud strikes, the losses are normally considerable, while the client’s reaction ranges from unfiltered anger to sheer disbelief that their bank “allowed” wire fraud to happen.

Criminals like wire transactions for many of the same reasons that clients do. Initiating a wire requires minimal effort and the funds appear within hours in the recipient’s account, ready for immediate withdrawal. There is theoretically no limit on the amount of a wire. If the funds are available, a wire transaction is an option.

Convenience, quick fund availability and no limit on the amount of the transaction — cybercriminals would be foolish not to target this payments channel.

Throughout the year, numerous examples of wire fraud appear in the business press and several of those cases have made it to court. How big is the problem and what can banks do to minimize the risk?

This paper provides an overview of wire fraud, including the tools and tactics cybercriminals use, a review of recent court cases and general approaches to help financial institutions combat the threat.

EXECUTIVE SUMMARY

The Cybercriminal: Tools and Tactics

Today’s cybercriminal has an impressive arsenal available to commit bank fraud. Just like legitimate companies, criminals employ different approaches based on their core competencies, sophistication and available resources.

Typically, wire fraud schemes fall into three main categories:

Scenario #1 – “I AM WHO I SAY I AM.”

Given the vast amount of data captured by companies around the globe, coupled with the frequency of data breaches — many of which do not make the news — criminals often have the data they need to take over a customer’s bank account entirely.

When the criminal initiates a wire transfer request, they have all of the information they need to pass the “call back” test, where a bank employee calls to verify the legitimacy of the transaction. Not only can the fraudster intercept or divert the call, he or she can also impersonate bank officials or a customer, allowing him or her to authenticate the payment instructions. Once the bank employee verifies data provided by the criminal as accurate, the bank sends the wire transaction which is subsequently “layered” (a series of complex transactions designed to eradicate traces of the original source) with the funds, eventually finding their way to the fraudster’s account. Retracing the money laundering process is impossible since
the cybercriminals deliberately move funds to and within banking systems that provide legal protections designed to shield the identity of account holders and their banking activity.

**SCENARIO #2 – “PLEASE VERIFY YOUR INFORMATION.”**
When it comes to stealing or tricking individuals into providing their personal information, cybercriminals are highly adept at leveraging all manners of technology for this purpose. The following tactics represent some of the more frequently used approaches that fraudsters use to gather data to commit wire fraud.

- **Phishing:** Emails purporting to be from legitimate companies with the goal of “trick[ing]” recipients into providing personal information. To provide information, the email normally redirects the recipient to an official looking site controlled by cybercriminals. Many individuals are often fooled into accepting fraudulent wire transfers and end up becoming money mules, which includes moving money on behalf of the fraudster. Other email scams trick individuals into thinking they are making investments (through wire transfers) with legitimate investment companies. These “companies” often look legitimate and trustworthy.

In some cases, the recipient is just plainly tricked into providing personal information on the promise of getting money (think Nigerian 419 advance fee email scams: “send me a processing fee and you’ll get lots of money as a payout”).

- **Spear phishing:** Emails targeting specific companies, departments or individuals requesting that the recipient share their personal information. To add legitimacy, cybercriminals may show a senior executive within the company as the author.

- **Denial of service/distributed denial of service:** Denial of service and distributed denial of service both attempt to overwhelm a bank’s servers, therefore blocking legitimate users from accessing the site. Whether fraud or data theft results before, during or after an attack is the subject of debate.

- **Watering holes:** A cybercriminal compromises a third-party site with malware. Visitors to the site inadvertently download the malware, which in turn enters their employers IT environment and infects its machines. The presence of malware may allow criminals to capture personal information, banking credentials or the company’s intellectual property.

- **Insiders:** A well-placed employee within a bank can do untold damage. Frontline tellers, for example, typically have unfettered access to customer information, including their current balance, contact information and normal account activity. In addition, bank employees often have the ability to change the customer contact information without additional oversight or approval from a member of management.

**SCENARIO #3 – “YOU’RE THE ONLY ONE THAT CAN HELP.”/“I’M ABOUT TO MAKE YOU RICH.”**
A customer receives an email from a “friend”, or at least someone they know, that apparently is in trouble. Typically, the friend is facing a life-threatening event that they can avoid if the customer wires them money. Since the email is supposedly from a friend and includes a sense of emergency, customers do fall for this type of fraud and wire the money.

There are a number of variations on this type of fraud, including schemes from apparently respectable members of society in foreign countries with the ability to secure vast sums of wealth if the email recipient provides a modest investment to start the process.

**FIGHTING WIRE FRAUD: THE FINANCIAL INSTITUTION’S PERSPECTIVE**

Customers demand convenience. They expect that their financial institution will allow them to access their account whenever needed, from whatever device they choose. Whereas 10 years ago, most customers appreciated logging on via their personal computer, today they expect to access their account from their personal computer, as well as their mobile device, including their phone and tablet such as an iPad.

As the number of devices that a customer uses increases, so too does the inherent complexity of verifying that the individual accessing their account online is the actual customer and not a member of an organized crime syndicate.

For example, if a customer uses their new phone to access their account, but mistypes their password several times and requests a new password, how can the bank know for sure that the customer initiated the request?
As we learned earlier, cybercriminals possess an array of tools to gather a customer’s personal data. The fraudster’s ability to gather the information they need appears to be as limited as their imagination. Although their use of the information is criminal and not to be condoned, their ingenuity is certainly astounding.

To complicate matters further, not all fraudsters employ the same techniques. Yet, financial institutions must have the people, processes and technology in place to respond to attacks, regardless of their origination, sophistication and frequency. Although harsh, there is no defense in the eyes of the customer for allowing fraudsters to steal.

Additionally, some cybercriminals specialize in acquiring data, while others focus their efforts in using the data to commit fraud, while others handle the entire operation from data gathering, usage and subsequent laundering of the proceeds. Just like “regular” companies, fraudsters develop core competencies that they use to create sustained competitive advantage, or in this case, the ability to overcome a bank’s fraud defenses.

In fact, criminals often seek to move money offshore or to other jurisdictions, knowing this makes recovery expensive and difficult for banks and law enforcement, as they have to work within legal boundaries. Organized crime does not have these same constraints. Civil actions by customers and banks are also expensive. Recovery of funds by customers and banks is usually drawn out and there is no guarantee that any money will be recovered. This only exacerbates the complexity of the issue.

Not surprisingly, given the inherent complexity of detecting and preventing wire fraud, when losses result, the customer and the bank often disagree as to who is at fault, and ultimately facilitated the fraud.

To avoid adverse publicity and the alienation of profitable clients, “behind the scenes” financial institutions may elect to reimburse the client for their losses. By doing so, banks avoid the cost and adverse publicity associated with litigation, as well as avoid the disclosure of the points of failure within the bank’s walls that may have allowed the fraud to take place.

However, making clients whole for wire-related fraud losses is a short-term solution that does not address the root cause of the loss. In most cases, cybercriminals took advantage of weaknesses on both the bank’s and the customer’s systems and online banking practices. Deciding which entity should shoulder the blame, and consequently the loss, is the job of the courts. In the following cases, the respective courts viewed the cases and arrived at differing opinions.

**CHOICE ESCROW AND LAND TITLE LLC VS. BANCORPSOUTH INC.**

In a dispute dating back several years involving an unauthorized wire of $440,000, the court sided with BancorpSouth. Cybercriminals stole the company’s login credentials and sent the wire to a corporate account in Cyprus. The bank previously offered the company dual control (two individuals must login and approve the sending of a wire), and the company declined. In addition, the company also declined imposing restrictions on the amount and frequency of wires permissible each day.

**Verdict:** The bank wins the case, primarily due to the customer’s refusal to implement additional security controls.

**PATCO CONSTRUCTION COMPANY, INC. VS. PEOPLE’S UNITED BANK**

Several years ago, fraudsters captured a Patco employee’s login, password and answers to security-related questions. Via six wires, cybercriminals withdrew $588,851, of which $243,406 was recovered. The parties settled after protracted litigation. People’s United agreed to pay Patco for losses it suffered. Originally, Patco sued for losses, damages and legal fees.

**Verdict:** The company settles with the bank after years of costly litigation for both sides.

**VILLAGE VIEW ESCROW VS. PROFESSIONAL BUSINESS BANK**

After suffering a $393,000 net loss associated with 26 fraudulent wires, Village View Escrow sued Professional Business Bank. The owner of Village View Escrow stated that the bank normally notified her via email of each wire transfer associated with her account. The fraudsters apparently disabled this service before launching their attack. Prior to the attack, the owner of Village View Escrow, Michelle Marisco, received an unsolicited email regarding an undelivered UPS
When she opened the attachment included in the email, nothing happened. She subsequently sent the email to her assistant, who also opened the attachment. The attachment was a Trojan horse that captured Marisco’s bank login credentials as well as her assistant’s. Using the captured passwords, the fraudsters provided two levels of approval required by the bank to release a wire. In order to allow access to its online banking channel, Professional Business Bank reportedly used single-factor authentication instead of multi-factor authentication.

**Verdict:** The bank agrees to reimburse the company for the loss and pay its legal fees.

**EXPERI-METAL VS. COMERICA**

District Court in Michigan rules in favor of Experi-Metal for $561,399 in losses associated with a phishing attack. The judge determined that Comerica “had not operated in good faith with respect to its online banking protections”.

**Verdict:** Comerica reportedly settled with Experi-Metal for an undisclosed amount.

As with any legal dispute, the application of the law to complex matters is an inexact science. Normally, both parties believe that the facts are on their side, yet for one party to prevail, the other must lose in some shape or form.

Legal action can result in compromise in the form of agreed upon settlements that take the matter out of the hands of the judge and jury to decide. However, regardless of the final verdict, both sides will undoubtedly spend considerable time and expense in and out of court pursuing the issue.

To complicate matters further, security measures available and commonly in place to protect consumer versus commercial accounts differ, as do the banking rules and regulations governing each type of account, and the corresponding liability for fraudulent transactions. Ultimately, when a customer sues its bank, no one really wins. Litigation of this type is rarely a “for profit” pursuit, and as these cases show, winning in a court of law is never a “sure thing”.

Like most types of bank fraud, combating wire fraud requires a proactive and vigilant multi-pronged approach, which acknowledges that certain elements of a bank’s defenses will fail, while the cybercriminal will overcome others. Relying on one control or set of controls to stop all wire fraud attempts is unrealistic and destined to failure.

Banks must continually adapt and readapt to the threat of wire fraud. Just because today a bank’s wire fraud losses are low is no guarantee that they will remain so. Cybercriminals pursue the “path of least resistance”. If a bank’s defenses are more robust than a competitor, and consequently more time consuming to overcome, chances are that fraudsters will focus their immediate efforts on the competitors that have weaker controls in place.

However, complacency will invite fraud in the future. Cybercriminals will continue to invest the time, energy and expense probing your bank’s defenses for weaknesses. Once uncovered, they will arrive in force and disappear as quickly and quietly as they arrived.

Fraud prevention tools typically focus on one or more of the following components associated with a customer’s account activity:

- **Authentication:** Involves the comparison of data gathered from the customer such as user name, password and something only the user knows (their dog’s name, for example) against information previously provided during the account opening phase, or at some point during the life of the account. Additional factors may include tokens that generate random numbers the customer inputs, a USB device that contains login credentials, or information about the customer’s computer device that the bank captures and associates with the account.

- **Account maintenance:** To open a new account as well as comply with “Know Your Customer” requirements, banks capture data regarding the customer such as name, address, phone number, email address, date of birth, etc. In the event that a customer changes elements of their data, such as their phone number or email address, the bank initiates a process using previously designated
communications methods such as mobile phone or secondary email address to confirm the customer did in fact make the request. The message sent may include a one-time password or a prompt to provide a “factor”, such as the information captured during login. In limited circumstances, the bank may call the customer to confirm the change.

• **User behavior:** How a customer interacts with a bank’s online site can follow patterns. For example, consider a retail customer that normally checks their account balances in a certain order, never initiates transaction online and always logs in from their desktop based in their home. In the event that they log in and initiate 10 ACH transactions using an unrecognized device that appears to be in France, software flags the account for further review. Similar behavioral profiling can be applied to monitoring business or corporate accounts.

• **Transaction monitoring and authentication:** Software reviews a customer’s comprehensive banking activity — regardless of the channel used by a customer — for red flags indicative of fraud. For example, a wire request to send money from a retail account with a large balance and very little transaction volume to the Caribbean may signal fraud. In addition to the destination for the funds, anomaly detection software captures considerable data corresponding to the transaction including the date and time requested by the customer, the payee account and name, the account number, the method used to initiate the wire and the level of authentication received by the bank. If, for whatever reason, the bank suspects that the wire may be fraudulent, they may contact the customer directly to confirm the request. Unfortunately, the individual they reach may in fact be the fraudster that changed the customer contact information to their own to commit fraud.

• **Analytics:** Sophisticated fraud threats often require sophisticated detection techniques. As fraudsters get more creative and bold, modeling techniques today are adapting to a tremendous increase in possible counter-measures. Financial institutions often turn to advanced predictive analytic techniques to detect virtually all types of financial crime. Custom built (using the institutions own known fraud data) or consortium (using the collective data of many institutions) approaches can provide extra protection in preventing such fraudulent activity.

For as long as banks offer their clients the ability to wire funds, cybercriminals will continue their efforts to commit fraud.

When banks and their customers disagree as to which entity should bear the burden of the loss, the dispute can end up in court. How courts apply the law relating to online fraud is open to wide interpretation. Consequently, neither party to a lawsuit can predict with any degree of certainty the chances of proving their case and receiving a judgment in their favor.

As with most types of fraud, prevention and detection requires a detailed understanding of the schemes fraudsters employ, and multiple layers of security that slow, frustrate and ultimately repel attempts to steal funds.

ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI's private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.