Dissecting Wire Fraud: How it Happens, and How to Prevent It
Introduction

Preventing wire fraud starts with understanding how it is perpetrated and the many options fraudsters have for initiating fraudulent wire requests. And it is indeed the money movement method of choice with 76 percent of all fraud attempts featuring a wire transfer, according to an FS-ISAC survey.

In the last 20 years, the number of wire transfers taking place has nearly doubled, now exceeding 130 million each year, while the total dollar value of all transfers has tripled in the same time period reaching $600 trillion in 2012.

The increase in originators, volume, and dollar amount and other inherent characteristics of wire payments make them very attractive to fraudsters. Financial institutions must shore up their security to decrease fraud losses and the accompanying operational and reputational costs. Controls designed to ensure the originator and beneficiary are legitimate are routinely defeated. And rules-based solutions being implemented by many institutions to detect fraudulent wires are time-consuming to set up and maintain, generate a large number of false positives, and still miss fraud.

This paper provides examples of actual fraud cases that illustrate the breadth of schemes in play, available fraud prevention solutions, and the strengths, weaknesses, and limitations of each. It also recommends a behavior-based fraud prevention strategy that has been proven in the marketplace to detect wire fraud regardless of how the wire request was originated or what fraud scheme is in play.
Fraud Schemes Use a Diverse Mix of How Accounts are Compromised, Points of Compromise, and Wire Initiation Method

Limitless Options For Committing Wire Fraud
Criminals constantly are evolving their schemes and attack vectors, not only mixing the methods and points of compromise and channels in new combinations, but also showing a growing trend of using online accounts in particular to gather information needed to commit fraud in other channels. Guardian Analytics’ own data has revealed thousands of fraudulent sessions where data was gathered online and used to perpetrate fraud in an offline channel.

Collectively, there are endless paths from the initial account compromise to the wire transfer, using both human and malware-based attacks to access accounts (see Figure 1).

Figure 1: Each path represents a different potential scheme, further complicated by the multiple variations within each node, such as the many malware families and variants.
Method of Compromise

Credentials and the accompanying personal information needed to compromise accounts are readily available on criminal online marketplaces. In addition, account holders not only still are using simple passwords, but they also are reusing the same passwords on multiple services, which makes it even easier for criminals to compromise accounts. When a fraudster compromises an email account, for example, there’s a good chance he also now has the password for online banking. A 2012 study of Yahoo and Sony breaches revealed that 60% of users that maintained accounts on both sites used the same password.

If the fraudster doesn’t have the credentials for his target victim, there are many options for acquiring them.

- **Malware** – It’s everywhere and therefore nearly impossible to avoid, distributed in email, on spoofed websites, and arriving in text messages sent to smartphones. There are an estimated 70,000 variants released every day. According to the Anti-Phishing Working Group, 40% of computers already are infected with malware. Rapid malware innovations create new threats and extend the time to detection, leaving FI’s further exposed. Malware detection providers themselves say that when something new appears, it can take weeks to research and formulate new protections. Criminal networks are sharing successes, technologies, and techniques, accelerating their investments to exploit this weakness.

- **Social Engineering** – A recent Gartner report described “fraud scams that took social engineering tactics to new heights of deviousness.” Criminals get credentials or other personal information from prospective victims and trick innocent 3rd parties, such as customer service agents, to actually help them complete a fraudulent wire.

- **Phishing** – Traditional phishing attacks start with an authentic looking email from a bank, a credit card company, the IRS, or another credible entity asking the victim to provide personal or financial information. The victim clicks on a link that goes to a fake site that collects personal or financial information, or the link installs malware on the victim’s computer.

- **Vishing & SMishing** – In vishing attacks (voicemail phishing) the criminal calls claiming to be a bank, credit card company, or similar organization (often achieved by spoofing the caller ID so it looks like the call really is from the bank), and asks the victim to confirm personal information over the phone. It’s either a live conversation or urgent sounding voicemail asking victim to call back and leave information to avoid some dire results. Fraudsters also use phishing attacks against mobile devices and tablets (SMS phishing, or SMishing), delivering a convincing and similarly urgent text message either with a link to a malicious payload or with a call-back number. When the victim calls, they’re connected to an Automated Voice Response (AVR) system that asks them for personal or financial information.

- **Email Compromise** – This works two ways: gaining access to email can lead to online banking access, and visa versa. Either way, the fraudster ends up with access to both systems. What makes it much easier for the criminals is account holders’ tendency to reuse passwords. When a criminal compromises a victim’s email account through other means, he has a reasonably good chance that the online banking password is the same as or very similar to the email password. In addition, compromising an email account provides criminals with access to personal information that could be used to successfully authenticate him in a range of online accounts and services.
Point of Compromise
As shown in Figure 1, each of these methods of compromise can be used against multiple targets, ranging from the account holder’s online or mobile device to customers themselves to bank employees.

Method of Wire Initiation
How an account is compromised does not necessarily dictate the channel through which the fraudster originates a wire. After obtaining credentials and compromising an account, fraudsters can submit wire requests through online and mobile banking channels as well as through offline channels such as the call center, fax, or through a branch.

Sample Fraud Schemes Featuring Wire Payments
The wire channel clearly is the money movement channel of choice for fraudsters, especially when one considers that wires are often used to move large sums, are frequently used by businesses that have large account balances, move money quickly, and are hard to reverse. To illustrate the point made in Figure 1, here are just a few of the many ways for criminals to originate fraudulent wire transactions. These examples highlight how fraudsters are able to bypass controls and defeat security measures.

Online Wire Request to Defeat Out-of-Band Confirmation – The most common wire scheme starts with compromising an online account and then either disabling all security alerts or entering a new phone number or email address, defeating out-of-band (OOB) confirmation and preventing the victim from knowing that the account has been compromised. The fraudster then simply submits a wire request through the compromised online account and approves his own request.

One specific technique to defeat OOB is to compromise the victim’s online banking account and change their email address to a very similar disposable email address (see Without a Trace Fraud Informer), which doesn’t look particularly suspicious but results in the confirmation email being sent to the fraudster.

Funeral Scheme Uses Compromised Email Account – The basic version of this scenario starts with the fraudster compromising the victim’s email account. He then uses the compromised email account to send a request to the FI’s relationship manager explaining that he’s out of country for a funeral and needs money for expenses. The FI emails the necessary Letter of Authority, which the fraudster receives, signs and faxes back, preying on the fact that FIs don’t check signatures carefully. Upon receiving the signed form, the FI wires the requested funds to the fraudster’s account.

A more sophisticated version starts when the fraudster compromises an online banking account to view check images to get the victim’s signature. The rest of the scheme unfolds the same as above, although this time the form is returned with an accurately forged signature. This scheme could also use other life events, for example an accident where medical expenses are the excuse for needing the funds.

Online Live Chat Targets Customer Service – A fraudster compromises an online banking account and gathers (or changes) personal information. He then engages in a live chat session with a customer service agent saying that he’s having trouble sending a wire and asks for help. The agent believes the fraudster
is legitimate because he has successfully logged into online banking. If the agent does request additional confirmation, the fraudster has gathered enough personal information to convince the agent that he is the real customer. (*see Chatting for Dollars Fraud Informer* for a complete write-up of this scheme.)

Commercial Account Takeover to Defeat Dual Controls – There are several versions of how fraudsters are able to take over commercial accounts and defeat dual controls.

1) A fraudster compromises an online banking admin account and then creates a new user with the authority to approve wire requests. He originates a wire request from the admin account, and then signs into the newly created account and approves his own wire request.

2) It also could work the other way, with the new account originating the wire and the admin account approving it, depending on what privileges the admin account has.

3) A third variation is that the fraudster modifies the privileges of the compromised account so that he can originate and approve a wire transfer from the same account.

Targeting Employees to Gain Inside Access to the Wire System – Using a spear-phishing scheme, malware designed to compromise the back-end payment system is installed on a bank employee’s computer. The malware takes over the victim’s computer, enabling the fraudster to submit a large-dollar transfer into the wire system (*see 2012 FBI alert*). This clearly is a more sophisticated attack, but the ability to steal a large amount of money makes it worth the effort to the fraudster.

Using DDoS Attack as a Smokescreen – The OCC has reported confirmed examples of DDoS attacks being used as smoke screens for fraud attacks (*read the alert*). One example is that the fraudsters contact customer service during a DDoS attack to ask for help completing a wire. The customer service agent is aware of the website being down and therefore is particularly eager to help, possibly bypassing some established security procedures and confirmations.

Template Modifications Are Nearly Invisible – This scheme starts with compromising the computer of an employee in the finance department or a corporate online banking account. In both scenarios, the objective is to locate existing wire templates and then modify the beneficiary information, possibly just the account number. These can be templates stored on a corporate server or employee's computer, or available through the company’s online banking account. After changing the template, the fraudster simply waits for the victim to use the template, hoping that they don’t notice the subtle changes that cause the funds to be wired to the fraudster’s account instead of to the intended beneficiary. In a variation on this scheme, the fraudster modifies the Originator-to-Beneficiary instructions (OBI) and inserts a request to forward the funds to an account that the fraudster holds (for example, he adds “for the benefit of” or “for further credit” instructions).

Fake Vendor Invoice – The fraudster mocks up a fake invoice from a known vendor and submits it to a company for payment with fraudulent payment instructions. Especially when the vendor being spoofed has a long-term relationship and is known to submit regular invoices, the victimized company often doesn’t review it quite as closely, but submits it to the bank for payment. Fraudsters will also use this scam to attack many companies simultaneously with the same invoice template, pretending to be a supplier used by a lot of different companies, such as the phone company or the electric utility.
Total Cost of Wire Fraud

While wire transfers themselves often are for large dollar amounts, the losses associated with a fraudulent wire don’t stop there. Additional costs incurred by the victimized financial institution include:

- **Investigation** – Time needed to research the loss, evaluate and possibly adjust internal procedures, and document the results. One financial institution estimates that it takes at least 100 person hours to complete an investigation into a fraud attack.

- **Remediation** – For corporate accounts, the financial institution is not legally required to reimburse the account holder for losses. But many do anyway in the interest of maintaining good customer relations and recognizing the lifetime value of the customer.

- **Litigation** – There are several legal precedents that side with the account holder that was victimized in a fraud loss. These results can increase the likelihood of victims pursuing legal measures to recover losses, resulting in legal costs for the financial institution.

- **Brand and Reputation Erosion** – Account holders have many choices for where to bank. So, the fact that a particular financial institution has been the victim of fraud impacts a prospective client’s decision on where to bank.

- **Fines** – Banks can face severe fines or penalties resulting from non-compliance. Often these fines are part of the public record and further erode the financial institution’s brand and reputation. Once a bank has been fined, the bank will be under closer scrutiny from bank examiners and may be required to submit more documentation or evidence of compliance for an extended period of time.

- **Customer Churn** – Despite best intentions and remediation, many customers still leave. A survey of small and medium-sized business conducted by Ponemon Institute found that 43% of customers took all or some of their banking business elsewhere after just one attack, even if there were no losses.

Available Solutions for Detecting Wire Fraud

There is a variety of solutions available designed to detect fraudulent wire payments. This section briefly describes each along with strengths and weaknesses.

**Manual Review**

The most basic fraud prevention strategy is to review all wire requests manually. While this can be tedious, especially reviewing details like account numbers that must be looked up and carefully checked, this strategy often is preferred by institutions that process a very small number of wires. The advantage is that there is no technology investment needed, but at the cost of staff time. And some fraudulent wires are very hard to distinguish manually from legitimate ones.

**Rules-based Solutions**

A number of solutions use rules to flag potentially suspicious wires. However, there are significant challenges presented by rules-based solutions that result in missed fraud, lots of time needed for maintenance, and a large number of false positives.
• **Requires knowledge of fast-changing fraud schemes** – Fraud schemes are dynamic. To write a rule to detect fraud, one must know what the fraud looks like, where the request originates, when it is likely to occur, or some combination of factors. But fraudsters continually change their tactics and have become good at disguising their true identity, location, beneficiary information, or other aspects of the attack that a rule might be written to detect.

• **Legitimate activities look like fraud** – Rules are written to detect unusual amounts or activities that could be indicative of fraud. However, what is unusual for one originator might be common for another, making it very challenging to write a rule that is effective against a diverse client base that likely has infrequent or dynamic wire activity.

• **False positives divert resources** – Rules-based solutions generate a large number of false positives. These are legitimate requests that still fail to pass one rule or another, and therefore require manual review before being processed. A large number of false positives requires staff time and increases the risk that, in their haste to keep up with the volume, someone will approve a request that truly is fraudulent.

• **Rules maintenance takes time** – Rules must be maintained; updated to reflect new policies, emerging fraud threats, or client feedback. It’s an endless process that is a steady drain on resources.

**Behavior-based Wire Fraud Prevention**

These systems model the behavior associated with wire payments and then compare all activity to the established baseline of normal behavior to detect unusual or unexpected activities that could be indicative of fraud. Behavior-based solutions have demonstrated their effectiveness at detecting fraud to the extent that the FFIEC included this as a minimum expectation of a layered security strategy (see page 5 of the Guidance issued in June 2011). While fraudsters have proven their ability to mimic the computer or location or IP address of an originator, they cannot mimic all aspects of normal behavior. At some point during the process of originating a wire, the fraudster will do something that is unusual or suspicious when compared to the victim’s normal behavior.

Behavior based solutions:

• **Automatically monitor the activity of every originator and beneficiary for every wire transaction**

• **Create and continually update models of individual behavior, comparing new wires to established norms for that particular originator**

• **Are easy to set up and don’t require rules to be established or maintained because behavior drives the model**

• **Focus manual reviews on only high risk wires, creating a minimal number of false positives**
Behavior-based Anomaly Detection – A Closer Look

Anomaly detection solutions detect unusual activity – anomalies – when compared to established norms. Behavior-based anomaly detection solutions do so while using individual originator, transaction, and beneficiary behavior as the focal point of what is being analyzed (see Figure 2).

**Behavioral Profile models normal behavior** – Behavior-based solutions create and continually update models of normal behavior that consider numerous characteristics of the originator, transaction, and beneficiary.

**Behavioral Analytics compares new wires to established norms** – All new wire requests are analyzed against the established models of normal wire activity as well as external fraud analytics and threat data. Additionally, behavior-based solutions:

- Analyze all wire requests from all channels, including those originated in a branch, via fax or email, through customer service, or directly from a customer.
- Alert only on items that are anomalous when compared to established normal behavior, and don’t generate alerts simply because a transaction exceeds a pre-determined threshold.

Figure 2. Behavioral analytics solutions use rich, historical activity information about the originator, transaction and beneficiary as well as external sources of threat data to analyze new wire requests in order to answer critically important questions and prevent fraudulent wires.
- Track and alert on even very small variances, such as changes to the beneficiary account number, while putting these small variances into the broader context of other factors and activities
- Allow FIs to employ limits and caps incrementally to behavior-based analysis to watch for specific high-risk activities or to accommodate specific client requirements

3. Resulting analysis detects fraudulent wires – Insights delivered help fraud and wire analysts answer critical questions to prevent fraudulent wires before they’re submitted for payment. The questions to be answered could include, are the originator’s actions normal, are the transactions typical, and are the beneficiaries risky?

Fraud Examples Revisited

Revisiting the examples of wire fraud described earlier, the chart below shows some of the suspicious activity in each scheme that would be detected by a behavior-based anomaly detection solution.

<table>
<thead>
<tr>
<th>Fraud Example</th>
<th>Activities Detected by Behavioral Analytics Solution</th>
</tr>
</thead>
</table>
| Online Wire Request            | • Unusual time of day for the request  
|                                | • Unusual amount of time since the last request (velocity) or frequency since prior requests  
|                                | • Unusual amounts and beneficiaries                                                                                   |
| Funeral Scheme                 | • First time originator and beneficiary  
|                                | • Inconsistent with prior wire requests  
|                                | • Looks suspicious in context of information from other banking systems; for example, recent online banking activity may indicate that the victim is not out of the country |
| Online Live Chat               | • First-time wire request  
|                                | • Unusual timing of the request  
|                                | • Unusual velocity  
|                                | • A new beneficiary  
|                                | • Variation in how the account holder typically initiates wires (e.g. typically it’s done personally and this time it’s through a bank employee) |
| Commercial Account Takeover    | • Unusual beneficiaries and amounts  
|                                | • Suspicious timing or velocity relative to previous wire activity                                                    |
| Inside Access to the Wire System | • Unusual beneficiaries and amounts  
|                                | • Suspicious timing or velocity                                                                                       |
| Template Modification          | • New beneficiary  
|                                | • Unexpected relationship between originator and beneficiary                                                          |
| Using DDoS Attack as a Smokescreen | • First-time wire request  
|                                | • Unusual timing of the request  
|                                | • Unusual velocity  
|                                | • A new beneficiary                                                                                                  |
| Fake Vendor Invoice            | • New payment details, such as the account number  
|                                | • Unusual velocity of payments to that vendor/beneficiary                                                            |
Advantages of Behavior-based Solutions

In addition to the most important benefit – preventing fraudulent wires – there are other advantages to implementing a behavior-based anomaly detection solution.

**Reduce Operating Costs** – Spend less time manually reviewing wires that pose no risk. Behavior-based solutions integrated with the wire system can automatically release low-risk wires, focusing efforts on the high-risk wires while providing the tools to quickly investigate and determine the most appropriate action.

**Reduce Customer Call Backs** – Rather than calling all customers submitting wires over a set dollar amount, FIs can reduce the number of outbound verification calls and limit them to the truly high-risk wires regardless of the dollar amount.

**Improve Client Service** – With the confidence that a behavior-based anomaly detection solution is monitoring all wires and will detect high-risk activity, FIs can improve client service by offering expedited or real-time wire processing.

**Improve Competitiveness** – FIs can attract new account holders by offering the fast, flexible wire payment services they’re looking for.

**High-fidelity Fraud Detection** – Typically rules are about the originator. Anomaly detection solutions look at originator plus the beneficiary behavior and history and the relationship between the two, which provides a better indicator of normal versus fraudulent activity.

Conclusion

It’s more important than ever for financial institutions to implement cost effective wire security solutions, especially considering the characteristics of the wire channel that make it so appealing to criminals, the sophistication and extensive capabilities of fraudsters, and the many ways in which they can use wires as part of their schemes.

Using behavioral analytics to understand originator and beneficiary behavior has proven its effectiveness regardless of how a wire request is originated, how an account is compromised, or the overall fraud scheme in play. Somewhere during the process of accessing an account, and setting up and submitting a wire request, the fraudster’s behavior will differ from the victim’s, at which point the financial institution can intervene and disrupt the transaction before any money (or time or trust) is lost.
About FraudMAP Wire

FraudMAP Wire is Guardian Analytics’ industry proven behavior-based fraud detection solution that detects fraudulent wire transactions originated from any channel – online, fax, email, call center, or in a branch—and across all types of wires—inbound, outbound, book and transfer. FraudMAP Wire integrates with all major wire platforms to analyze each wire transaction, and automated risk scoring creates a streamlined workflow for managing wire risk.

FraudMAP Wire uses proven behavior-based anomaly detection capabilities to identify high-risk wire activity, resulting in maximum detection with a minimum of false positives, all without manual intervention or rules to write and maintain. Using Guardian Analytics’ proprietary and patented behavioral analytics technology, Dynamic Account Modeling®, FraudMAP Wire creates and dynamically updates behavioral profiles for each wire originator and beneficiary. FraudMAP Wire analyzes each wire to determine if there is any anomalous activity relative to the typical behavior. Each wire is analyzed against a wide range of prior account activity such as frequency, velocity, originating channel, originator and beneficiary information, business function code, destination location, method of payment, amount, timing, and more.

With FraudMAP Wire, financial institutions can prevent fraudulent wires, reduce the costs of manual wire reviews, and offer expedited wire services.

About Guardian Analytics

Guardian Analytics is the leader in behavior-based anomaly detection solutions for preventing fraud. The result is banks and credit unions that have the confidence to offer the banking services their clients want while protecting their assets, reputation, and trust. Hundreds of banks and credit unions and millions of account holders rely on Guardian Analytics to protect individual and business account assets. To learn more about Guardian Analytics and FraudMAP Wire, please go to www.GuardianAnalytics.com.