Stopping the Flow of Stolen Money:
Using transaction monitoring to stop online banking fraud.
With cyber crime increasingly impacting small business in America, it is important to consider how criminals continue to move stolen funds. The face of online banking fraud is continuously changing, yet there is one obvious constant: the transaction. No matter how criminals change their approach, and no matter how patterns of computer hacking change, the money has to be moved out of one account and into another.

Money mules play a central role in moving illegally obtained funds through online banking fraud. Whether a willing participant in the crime or an unwitting scapegoat, the person playing the role of money mule is most directly in the line of fire and increasingly paying the price for their role in the crime. This is perhaps why it is becoming increasingly difficult for criminals to recruit American-based money mules.

This white paper argues that online banking fraud is constantly shifting. Even the traditional role of the money mule is changing. The most effective and efficient means to stopping online banking losses is behavior-based software that applies progressive analytics to back-end transaction monitoring. Most importantly, the monitoring results in alerts that help fraud detection professionals stop transfers before the money is gone.

What is a money mule?

The Oxford Dictionary defines a mule, in part, as a “beast of burden”. This is also an accurate way to describe the animal’s symbolic counterpart in modern day financial crime, the “money mule”.

Quite simply, “money mule” is a derogatory term to describe a person that, in the course of a financial crime, carries the money. He owns the account that receives the stolen funds and then moves the money to a location where the fraudster can safely access it. Essentially, he cleans the dirty money in return for a small commission.

Tell me more.

The mule is the lynchpin. Strictly keeping within an online banking fraud context, the flow of the crime works like this: the cyber criminal illegally accesses an account, such as through the use of a stolen password, or the installation of a virus on the victim’s computer, and moves money out. That money has to go to an account that is not obviously associated with the criminal. Enter the mule. The criminal has coerced a
A recent Microsoft Research paper authored by Cormac Herley and Dinei Florencio, entitled “Is Everything We Know About Password-Stealing Wrong?”, argues that mules are “the true victims in credential theft fraud.” Consider the rationale for their argument. A victim’s account is hacked and the money is moved to a mule’s account. The majority of that amount is then moved to the criminal’s account, often overseas. Since consumers are protected from online banking fraud losses by Regulation E (a consumer protection measure issued by the Board of Governors of the Federal Reserve System), the bank initially looks to the mule’s account to make the victim whole. In turn, the mule loses any

A high-level visual of a corporate account takeover.

While corporate account takeover has become increasingly complex, the following graphic provides a visual for the basic flow of online banking fraud.

What is this recent talk of the mule being a victim?

A recent Microsoft Research paper authored by Cormac Herley and Dinei Florencio, entitled “Is Everything We Know About Password-Stealing Wrong?”, argues that mules are “the true victims in credential theft fraud.” Consider the rationale for their argument. A victim’s account is hacked and the money is moved to a mule’s account. The majority of that amount is then moved to the criminal’s account, often overseas. Since consumers are protected from online banking fraud losses by Regulation E (a consumer protection measure issued by the Board of Governors of the Federal Reserve System), the bank initially looks to the mule’s account to make the victim whole. In turn, the mule loses any
There is a lot of talk about how the mule is the bottleneck in the financial crime process. Elaborate networks are being set up to recruit more and more mules. Brian Krebs, who maintains a security news and investigation blog (krebsonsecurity.com), writes that a mule is worth approximately $10,000 to cyber thieves. His calculation considers that, to avoid suspicion, the thieves generally transfer under $10,000 per mule account. In some cases, this value is higher when dealing with banks that they know will alert on larger transfers. Krebs’ own research has unearthed close to two dozen money mule recruitment networks. It is worth noting that the majority of these networks will demand 40-50 percent of the fraudulent transfer amounts. The fact that they can demand such a price indicates how difficult reliable mules are to find.

Much of this difficulty can be tied to the intense law enforcement effort currently focused on infiltrating and stopping mule networks. There are numerous examples across the country, such as Operation Texas Money Mule, a joint operation between the Texas Bankers Electronic Task Force and the Secret Service.

Indications are that these difficulties may be causing criminals to shift away from using mules. Recent activity suggests the newest mules may not be human at all, but plastic. Consider the recent online fraud attack on Alta East, a wholesale gasoline business in Middletown, New York. In March, a number of their employees received email messages enquiring about a recent business transaction. Each of the employees opened the attached PDF file, unwittingly installing a variant of the ZeuS Trojan virus on their computers. Up to this point we are hearing an all-too-familiar story. Here is where the story diverges slightly: six days later, the cyber criminals set up a batch of fraudulent payroll payments to create 15 Metabank prepaid cards. The rest of the funds were sent to traditional money mules.

How are things changing?

There is a lot of talk about how the mule is the bottleneck in the financial crime process. Elaborate networks are being set up to recruit more and more mules. Brian Krebs, who maintains a security news and investigation blog (krebsonsecurity.com), writes that a mule is worth approximately $10,000 to cyber thieves. His calculation considers that, to avoid suspicion, the thieves generally transfer under $10,000 per mule account. In some cases, this value is higher when dealing with banks that they know will alert on larger transfers. Krebs’ own research has unearthed close to two dozen money mule recruitment networks. It is worth noting that the majority of these networks will demand 40-50 percent of the fraudulent transfer amounts. The fact that they can demand such a price indicates how difficult reliable mules are to find.

Much of this difficulty can be tied to the intense law enforcement effort currently focused on infiltrating and stopping mule networks. There are numerous examples across the country, such as Operation Texas Money Mule, a joint operation between the Texas Bankers Electronic Task Force and the Secret Service.

Indications are that these difficulties may be causing criminals to shift away from using mules. Recent activity suggests the newest mules may not be human at all, but plastic. Consider the recent online fraud attack on Alta East, a wholesale gasoline business in Middletown, New York. In March, a number of their employees received email messages enquiring about a recent business transaction. Each of the employees opened the attached PDF file, unwittingly installing a variant of the ZeuS Trojan virus on their computers. Up to this point we are hearing an all-too-familiar story. Here is where the story diverges slightly: six days later, the cyber criminals set up a batch of fraudulent payroll payments to create 15 Metabank prepaid cards. The rest of the funds were sent to traditional money mules.
In January 2012, the FBI posted information about the “Gameover” malware on their website. With this malware “strain”, a person typically receives an unsolicited email, allegedly from NACHA (the Electronics Payments Association), the Federal Reserve, or the FDIC indicating a problem with a recent ACH transaction. A link within the email brings the person to a site where they inadvertently download the “Gameover” malware, infecting their computer and stealing banking information.

Interestingly, investigations indicate that some of the funds stolen in recent related attacks have not been transferred into the accounts of money mules. The cyber criminals contact high-end jewelry stores, indicate specific goods they intend to buy (such as precious stones and expensive jewelry) and promise to wire the funds to complete the purchase. The next day, the mule goes to the store to pick up the merchandise. After verifying receipt of the money, the goods are given to the mule, who then hands the items over to the organizers of the scheme, or converts them for cash and launders the funds. This is another twist on the traditional funneling of stolen funds into a mule’s account that helps distance all of the players from the crime.

Proactively stopping the transaction.

As criminals attempt to change their approach, the need to transfer the funds out of the account remains constant. There is no obvious way around it.

The importance of investigating the transaction and proactively stopping it before the money is gone is at the foundation of Verafin’s approach to online banking fraud detection. This ability to stop the attempt to transfer funds is essential to stopping loss.

A little bit about Verafin.
Verafin is a behavior-based FRAML (Fraud detection + Anti-Money Laundering) software solution. It applies pattern recognition analytics and known fraud scenarios to customer transactions to detect anomalies. Out-of-the-ordinary behavior generates risk-rated alerts containing detailed evidence that indicates why the alert was created. The alert also contains a customer’s demographic information and their alert history. Further, from an alert you can access a customer’s profile that contains historical transaction data and an automated risk score based on their demographic and cross-channel transactional data.

All of this is tied together by a case management workflow that lets users effectively build and document their financial crime investigations in a centralized location.
A real life online banking fraud scenario.

Consider the following scenario, loosely based on an attempted online banking fraud incident that Verafin helped stop. It illustrates how Verafin helps to proactively halt online banking fraud losses.

ABC Trucking Inc. is a customer of XYZ Bank. They have 50 employees and use the bank’s online banking platform to perform payroll transfers.

Early in the week, Vanessa, one of ABC’s employees, receives an email from NACHA stating that there was a problem with a payment to one of the company’s suppliers. The message indicates that she can resolve the problem by clicking the support ticket link at the end of the email. Concerned that an issue with the supplier may cause delays in their upcoming product shipments, she clicks the link and is brought to a web page that indicates the support email was sent incorrectly and apologizes for the inconvenience. Happy there is no problem, Vanessa goes back to tackling her daily tasks. Unknown to her, she has just played a role in a phishing attack on ABC Trucking and infected her computer with Trojan malware.

Okay, this is a pretty familiar phishing scenario and one of the most common ways that cyber criminals are getting access to bank accounts of small businesses. Now, let’s consider how this scenario typically plays out across the country.

On Thursday morning, Vanessa attempts to log on to the account to complete the company’s payroll. Once she enters her credentials and one-time password, she is taken to a screen explaining that the website is currently undergoing maintenance and should be back online in 30 minutes. If she has any questions, she can call the bank’s support hotline at the number provided.

A typical payroll for ABC Trucking is $100,000. While Vanessa believes she is locked out of the account, the cyber criminals take over the account and change the account and routing numbers of 10 of the 60 employees on ABC Trucking’s payroll. The new numbers represent the accounts of money mules located in numerous other states. They also increase the amount being sent to these 10 accounts from approximately $2000 to approximately $9000 each. This only takes them minutes, and once done, they send the payroll file. It goes unnoticed because the criminals have nearly matched the standard payroll dollar total. Vanessa logs in after lunch on Thursday to send the company’s payroll. Shocked, she finds that she cannot send it because the company has reached its daily ACH limit. She calls the bank, but by the time they discover what has happened, the payroll is sent. A lot of frustration and anger is building towards XYZ Bank, as ABC Trucking immediately blames them for the loss.

Fortunately, this scenario can play out quite differently if XYZ Bank is using intelligence-based software to analyze transactions for anomalies.
After the criminals have altered the payroll information, the morning's ACH files are analyzed by Verafin before the funds are transferred. Judy, a fraud investigator at XYZ Bank, receives an email that there is a new online banking fraud alert generated in Verafin. She logs in immediately and sees the new alert with a very high risk rating (98).

She first checks the Evidence section of the alert and sees that Verafin discovered numerous anomalies that indicate a potentially “Hijacked Payroll”. Clicking the “Hijacked Payroll” evidence, she sees that the anomalies are “Excessive Average Payment”, “Altered Payees”, and “New Payees”. Clicking each of these scenarios, she sees the affected transactions. Within Verafin, she pulls up the company’s transaction history and contacts the customer. Now she can move quickly to stop the fraudulent payments.

Because Verafin detects anomalies before the ACH files are transferred to the Federal Reserve, Judy is able to stop the transaction before the money is gone. The bank informs a relieved and grateful ABC Trucking.

How Verafin helps.

After the criminals have altered the payroll information, the morning's ACH files are analyzed by Verafin before the funds are transferred. Judy, a fraud investigator at XYZ Bank, receives an email that there is a new online banking fraud alert generated in Verafin. She logs in immediately and sees the new alert with a very high risk rating (98).

She first checks the Evidence section of the alert and sees that Verafin discovered numerous anomalies that indicate a potentially “Hijacked Payroll”. Clicking the “Hijacked Payroll” evidence, she sees that the anomalies are “Excessive Average Payment”, “Altered Payees”, and “New Payees”. Clicking each of these scenarios, she sees the affected transactions. Within Verafin, she pulls up the company’s transaction history and contacts the customer. Now she can move quickly to stop the fraudulent payments.

Because Verafin detects anomalies before the ACH files are transferred to the Federal Reserve, Judy is able to stop the transaction before the money is gone. The bank informs a relieved and grateful ABC Trucking.

The transaction is the common denominator in a constantly shifting space.

The common denominator across all types of online banking fraud is the transfer of money that has to occur. What the cyber criminal does once he has access to the account changes depending on the opportunity: Does he watch the account over time, analyzing behavior patterns to avoid detection? Does he perform a smash-and-grab (accesses the account and transfers as much money as possible in seconds)? The criminal could do either. Is even the way criminals rely on money mules changing? What we know for sure is that the criminal needs to transfer the money out of the account. This is why back-end transaction monitoring software that helps stop a fraudulent transfer is such an important piece of the security puzzle.
Conclusion.

A layered approach to online security and online banking fraud detection is essential. Increasing levels of checks-and-measures frustrate criminals and make their task near impossible. However, each is prone to error. Consider the weakness of some commonly discussed security layers when they stand alone:

Customer education is essential. However, what a customer does is not something a FI can ultimately control. This is especially true for business/corporate customers where it is a matter of educating hundreds of employees, not just one person. Additionally, that education has to sink in and be used by every employee. One slip and the cyber criminal has the access he needs.

Authentication has time and time again proven to be fallible; any number of stories that detail account takeovers prove that criminals now easily navigate around this type of roadblock.

Monitoring account user activity after log-in is helpful but without the benefit of cross-channel transaction data has the potential to provide an incomplete picture. There is little room for delays in investigation when dealing with the speed of online fraud.

The last, and strongest, line of defense is transaction monitoring that alerts the FI to abnormal transfer behavior and allows the investigator to stop the transfer of money before it is gone. And that is perhaps the most important advantage: because Verafin analyzes an ACH transaction before it goes to the Federal Reserve, a FI can stop both the transfer and the loss.
Learn more.

To access Verafin’s ever-growing archive of webinars, white papers, success stories and other materials focusing on BSA/AML compliance and fraud detection topics relevant to financial institutions across the country, check out our Resource Center at www.verafin.com/resource-center.

About Verafin.

Verafin is a leader in fraud detection and anti-money laundering solutions for financial institutions, with over 850 customers that span 65 core processing systems and a broad asset range. Verafin helps financial institutions comply with the Bank Secrecy Act, USA PATRIOT Act, and FACTA regulations, while also helping to protect against fraud. Verafin is the exclusive provider of BSA/AML and fraud detection software for the California Bankers Association, Massachusetts Bankers Association, CUNA Strategic Services and 40 leagues and associations in the United States. For more information, visit www.verafin.com or call 1-866-781-8433.