Money mules

by Steve D'Alfonso and Brooke C. Satti

Contents

Executive summary

Money mules are in important element in the process of extracting money from compromised financial accounts. A money mule is a person who receives and transfers money acquired illegally on behalf of others and receives a commission in return. There are fraud schemes that do not require money mules; however, mules are needed by cyber criminals and international organized crime groups (OCGs) that focus their efforts on compromising bank accounts. Cyber criminals, often located in eastern European countries, require the help of accomplices located in the same country as the compromised victims to successfully "cash out" a compromised account. Mule "herders" who specialize in recruiting and organizing mule activity sell their services to international OCGs.

Mules are often recruited online through job advertisements and spam email. The job titles may include, but are not limited to, "payment processing agents," "money transfer agents," "loan processors," and "mystery shoppers." Mules also may be recruited through romance and lottery scams. Criminals trading in stolen or illegally acquired goods may need mules to receive packages and forward them to mail drops not traceable back to the criminal; this type of scam is known as re-shipping fraud.

The use of money mules is a low-risk activity for the criminal actors. They remain anonymous while the mules acting on their behalf run a high risk of arrest, conviction and jail time.

This paper provides a general overview of money mule types, recruitment methods, emerging threats and schemes, and red flag indicators of mule activity.

What is a money mule?

The term *mule* comes from the narcotics trade and refers to an individual who is paid a fee for transporting illicit drugs. The meaning of money mule is analogous, but different because typically no physical transporting of cash is involved. However, in some circumstances the mule will withdraw cash to provide to a representative of the criminal group or leave at a designated drop point.

Thus, a money mule is an individual who knowingly or unwittingly engages in the movement of illicit proceeds or goods for a commission. Money mules are recruited by criminal organizations or mule herders in various ways. Most often they are recruited through online advertisements and spam email for work-at-home and secret shopper jobs. The employment ads typically indicate that the job applicant will earn a good wage for little work with minimal skill requirements. Criminal groups also actively seek out candidates who have posted their resumes on job hunting websites. The job applicants are often put through an interview and evaluation process that adds legitimacy to the fictitious business that posted the position.

Money mules may be knowing (witting accomplices) or unknowing (unwitting accomplices).

- *Knowing mules:* Are fully aware of the scheme in which they are participating. They may not be malicious; for example they may be normally upstanding citizens who fell into financial hardship and suspect the activity they are about to engage in is illegal, but are desperate to earn money.
- *Unknowing mules:* Are unaware that they are participating in a criminal activity. They are often older, lonely or otherwise vulnerable adults who strike up relationships through online dating sites and other social networking sites and develop strong emotional ties to the fraudster. The fraudster, acting as predator, cultivates a dishonest personal relationship with the victim. Eventually, the fraudster will ask the victim for a favor that will involve the victim receiving and transferring money or goods.

Whom do mule herders target?

Mule herders need to find people who will respond favorably to unsolicited spam email or an advertisement touting the potential to work from home and earn sizeable income with minimal time commitment and no required skills. The people who meet that requirement tend to fall into one of three categories: gullible, desperate, or knowing.

The extremely gullible

Mule herders target people in the third of three tiers of gullibility:

- *Tier 1*: People in this tier will immediately identify fraud messages as suspicious. These people will typically delete a suspicious email without reading it or ignore the advertisement.
- *Tier 2*: People in this category may have their interest piqued and inquire further about the "opportunity" being presented. However, upon further review they will determine that it is suspicious and stop communication.
- *Tier 3*: These individuals are extremely gullible and trusting. They may be lonely individuals that need companionship and are easily drawn into a romance scheme. They tend to be easily persuaded and misled. Individuals in this tier will also view a fraudulent work-from-home scheme without suspicion and believe they have found a great opportunity. People in this tier are the target market for fraudsters, and elderly people in this tier are particularly susceptible to romance and lottery schemes.

The financially distressed

High, long-term unemployment in the US and other countries has left some people desperate for income. Individuals that are financially distressed may be frantic to make ends meet. The prospect of making several thousand dollars each month on a part-time work-from-home basis is too tempting for some to pass up. Many likely suspect they may be involved in a scam, but believe they have nothing to lose. Investigative journalist and blogger Brian Krebs interviewed more than 150 money mules and found that many opened new accounts, separate from their regularly used accounts, because the knew there was a possibility that they were entering into a scam.[2]

Knowing accomplices

In addition to the gullible and the distressed, mule herders may have access to knowing mules, otherwise known as a professional mules or mules for hire. These individuals are either working together with a criminal organization or being forced to commit the fraud against their will, for example, to pay off a debt.

Mule turnover and geography

Mules are often used just once and must continually be replaced. The mule selection process is simply a numbers game. Because of the low cost of email, fraudsters can send out thousands of spam messages hoping to get a few people to respond, and advertisements can be placed for free on sites like Craigslist. The economic recession has certainly aided fraudsters by increasing the supply of financially troubled people.

Great Britain and the eastern United States are key target areas. Their time zones are compatible with eastern Europe, which is where many cybercriminals operate. There have been money mules in the western United States, but they are a relatively rare by comparison with the east. Open source reports indicate that Singapore and areas within India have become popular with Nigerian criminal organizations over the last few years. In November 2013, the Singapore National Crime Prevention Council announced that through nine months of 2013, the police investigated 133 money mule cases compared to just 93 for all of 2012.[2]

Effects of money mule activity on financial institutions

There are several potential negative effects that money mule schemes can have on financial institutions (FIs). These effects are related to financial losses, regulatory fines, and reputational damage.

- *Financial losses:* Money mules are just one part of a wider cybercrime scheme to defraud FIs and their customers. Because many banks have zero liability policies related to customer online banking, the FIs typically absorb the losses.
- *Regulatory fines:* The specific actions taken by money mules to transfer or transport money to fraudsters constitute a money laundering transaction. FIs in the US, UK and other countries have faced increased regulatory scrutiny of money laundering activity over the last decade. FIs are expected to have a robust money laundering program and know-your-customer policies and procedures. Fines for noncompliance with anti-money-laundering regulations can be substantial.
- *Reputational damage*: FIs face damage to their reputations if they are caught in a widespread money mule syndicate or are frequent targets of money mules due to weak account opening controls. If such activities get press coverage, consumers may lose confidence in the FI. Conversely, FIs with strong fraud and money laundering monitoring systems and advanced analytical tools will be at an advantage. These institutions will be able to assist law enforcement and enhance their reputation by identifying money mule rings and fraud activity.

Schemes involving knowing money mules

The old-fashioned way a fraudster would recruit a mule was through real-world interactions. Low-level players in organized crime families or individuals looking to make profits quickly would be tasked with this role. Their job would entail moving money from point A to point B. These professional mules do still exist. However, tighter anti-money-laundering laws and regulations have become the norm and financial institutions have created methodologies to spot these instances. The role of the traditional professional mule is therefore much harder.

Organized crime groups adapted to this new environment by creating a number of schemes that employ unknowing money mules. The "professional" role changed from being an actual mule to being a mule herder. With technology and the internet, mule herders no longer have to rely on being within close proximity to mules to ensure their schemes are completed. "A single mule herder can run multiple mule operations, each focusing on a different country and language. If in the past most mules were accomplices, today they're mostly unwitting mules, regular Joes who get scammed into being mules and are not necessarily less innocent than the actual victims of the fraud."[3]

Professional mules

A professional money mule is someone whose main occupation is to receive and transfer money acquired illegally. These professional money mules or "mules for hire" are adapting to today's technological era and are utilizing commercially available crimeware to complete their fraud. Crimeware is a type of malicious software designed to carry out or facilitate illegal online activity.

One well-known case involved a cyber-ring of 70 money mules that defrauded millions of dollars from US and UK banks utilizing the Zeus trojan crimeware. The Zeus trojan operates through Microsoft Windows operating systems. It is used to carry out criminal tasks, steal banking information and install CryptoLocker ransomware.[4] It spreads through phishing schemes and malicious downloads.

The majority of the criminals involved in this ring were from Russia, Ukraine, Kazakhstan and Belarus and consisted of a mule organization, mule herders, individuals who obtained false passports and the mules themselves. While some of the individuals in this scheme were victims unaware of the fraud, the majority of the players were knowing parts of the operation. The controllers of the malicious trojan spread it to victims' PCs through e-mail. Once the victim's computer was infected, the malware allowed the attackers to steal the victim's banking information, thus allowing for the transfer of money from victims' accounts to mules' accounts. The mules would then withdraw the money and send it to their accomplices, keeping a small portion for themselves.

Another example of a professional mule situation is in auto auction fraud schemes. Criminal groups establish online auctions for cars or other merchandise that is non-existent. Victims that respond to the fraudulent listings are instructed to send payment to a mule account. The mule then transfers the proceeds overseas to his co-conspirators. One of the most well-known professional auto auction money mules is a Romanian, Adrian Ghighina, who pleaded guilty to wire fraud in 2011. He acted as a money mule for four years, moving around the U.S. opening bank accounts in fake names. The accounts were used to receive the illicit proceeds from victims of fraudulent auto auction frauds.[5]

J-1 visa mules

The US State Department's J-1 Visa Exchange Visitor Program[6] is a cultural exchange initiative. There are many sub-programs for such purposes as au pair work, visiting physicians, scholarly research and interns. It also includes the summer work travel and university student programs, which have been exploited by OCGs to recruit and place money mules within the US.

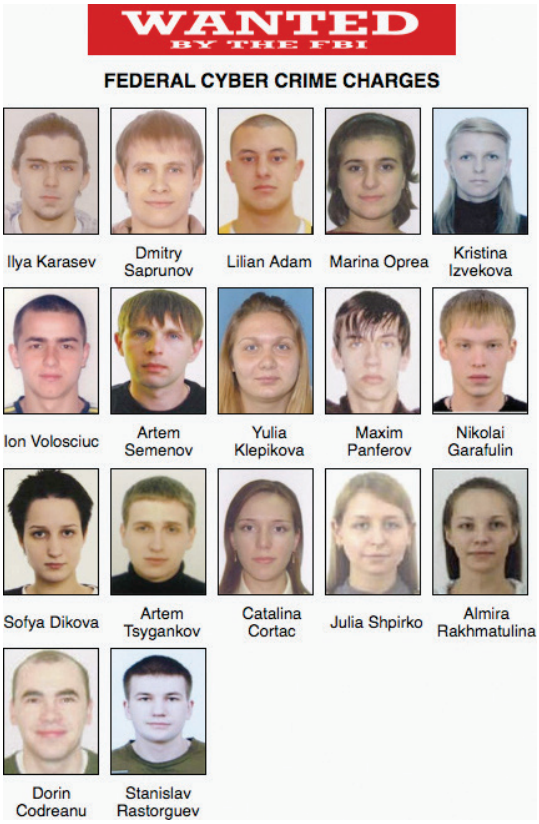

Figure 1: Individuals charged as part of the ACHing Mules investigation in 2010.

Source: FBI

In this type of scheme, young adults are recruited in their home countries through social networking sites, online advertisements and personal contacts to serve as money mules while working or studying in the US. The mules open an account and provide the account details to their handler or to the OCG. The OCG hackers use various online techniques to compromise the online banking credentials of consumers. Once compromised, the OCG may initiate an automated clearing house (ACH) transfer to the mule's account, who will then transmit the funds electronically to the OCG or will withdraw cash and smuggle it back to their home country for delivery to the OCG.[7]

Perhaps the largest and most famous takedown of a J-1 visa operation was Operation ACHing Mules in 2010.[8] As a result of the investigation, charges were filed in the Southern District of New York against 37 people acting as mules or mule herders (see Figure 1). The international fraud ring, based in eastern Europe, was responsible for stealing more than USD 3 million from small businesses and municipalities.

The ring used Russian social networks to recruit young adults who had J-1 visas. The mules were then provided fake passports. Once in the US, they opened bank accounts under aliases. The accounts were destination points for ACH transfers from compromised accounts. The illicit funds were sent back to eastern Europe via ACH, or the mules withdrew cash and smuggled it back.

Schemes for targeting unknowing money mules

Schemes that target unknowing participants are typically focused on employment and relationship scams. At some point the victims of these schemes, particularly the employment scams, may become knowing—or at least suspecting—mules. They realize that they may be part of an illicit scheme, but because of personal circumstances will continue to try and make money.

Work-from-home schemes

Work from home (WFH) schemes are fake job offers that are used by fraudsters and mule herders to entice individuals to provide bank account details for purposes of receiving an ACH deposit or counterfeit check. They are then instructed to electronically transfer funds to a third party, often in another country. Mules are also often instructed to make transfers to the third parties via a money service business, such as Western Union. Occasionally, mules will deliver cash in person to representatives of the crime group. In-person transfers usually involve a mule who is a willing participant to the illicit scheme.

WFH offers are usually cleverly created to look like legitimate companies. They will sometimes use recognizable trademarks, logos, or names to create apparent legitimacy. Fraudsters use two main methods to show these job opportunities to potential victims:

- *Spam email:* The emails are designed to look legitimate and bypass spam filters. The subject line is designed to entice people to open the email with claims such as "make thousands while working from home." Fraudsters often collect email addresses by trawling career sites to find individuals who are seeking employment.
- *Online classifieds and social networking sites*: Fraudsters will post job opportunities in the employment sections of sites such as Craigslist. The job application shown in Figure 2 is an example of what might be found online. The advertisement provides a description of the little work that is required to earn USD 500 per week. People who click on the website link will be brought to a page that likely looks legitimate, provides more information and has an application process.

The job application process for some opportunities requires applicants to be interviewed by a company representative and possibly sign an employment contract. One or both steps may be taken by the fraudsters to enhance the legitimacy of the offer.

Swatch Group Job Application

Greetings,

We would like to present you a part-time job offer as a finance officer for our company, Swatch Group. Our company sells deluxe watches in Europe and in some areas in United States. We would like to extend our business in your region, that is why this part-time job was created.

Processing a payment involves the following:
1. Receive the payment from our customers by Bank Transfers.
2. Pick up the payment from your account and keep your 10% commission fee.
3. Send the rest of the money to one of our headquarters in Europe.

This job will require about 1-2 hours per day from your time and your incomes will start from 250-300 USD per week to 500USD per week.

If you are interested in our offer please visit our website by clicking on the following link:

Click here to access our website

Thank you,
Swatch Group.

© 2011, **Swatch Group**, Switzerland.

Figure 2: Example of a fraudulent job posting

Source: nakedsecurity.sophos.com

Individuals that succumb to these types of fraudulent job offers are often financially distressed due to extended unemployment or other financial hardship. Unfortunately for them, most mules are only used once and may never see a commission. In addition, there is a significant chance of being arrested and even to be a victim of identity theft later on. This is because during the application process the fraudsters collect victims' personally identifiable information they need, including Social Security numbers.

The work-from home mule process

Assuming that an individual has received and responded to an email or a job posting, the remainder of the scam proceeds as follows:

- **The new employee (mule) will be instructed to provide bank account information or to set up a new account at their local bank and supply that information to the fraudsters.**
- **The mule will receive an electronic funds transfer (EFT) deposit into their account. The amount of the deposit will typically be less than USD 10,000.**
- **The mule will receive instructions about where to transfer the funds, minus a commission. The mule will then perform an EFT from that account or through a service such as Western Union or MoneyGram. The typical commission for the mule is 10 percent or less.**
- **The destination for the transfer may be to another mule or directly to a foreign bank account.**

A variation of this scheme is called a re-shipper scam. The recruitment process is the same, the only difference is the mule will receive illegally obtained merchandise and will be instructed to send that merchandise to a third party. Again, this recipient may be another mule or a criminal agent overseas. As compensation the mule is promised a commission, which never arrives.

These types of scams are successful because it may be difficult to distinguish between legitimate and illegitimate work-from-home opportunities. The US Computer Emergency Readiness Team provides the following warning signs of mule recruitment:

- The position involves transferring money or goods.
- The specific job duties are not described.
- The company is located in another country.
- The position does not list education or experience requirements.
- All interactions and transactions will be done online.
- The offer promises significant earning potential for little effort.
- The writing is awkward and includes poor sentence structure.
- The email address associated with the offer uses a web-based service (Gmail, Yahoo!, Windows Live Hotmail, etc.) instead of an organization-based domain.

Case example: work-from-home scam

A woman was on Craigslist looking for a job when she found a "work-from-home" administrative assistant opportunity. She applied for the job and that's when things took a strange turn. She had not yet accepted the position, yet a package arrived at her door containing a check for USD 3,450. Along with the check, the envelope contained detailed instructions to deposit the check into her personal ATM account, keep USD 400 for herself and send the rest via two separate MoneyGrams to different individuals in West Africa. This potential victim realized it was fraud and reported it. Read the full article here.

Secret shopper schemes

The secret shopper or "mystery shopper" mule falls victim to a scam similar to the work-from-home scheme previously discussed. It is an employment-based scheme designed to lure victims with offers that claim they can earn extra money for shopping at certain stores. In another variation, the shopper gets to keep the goods that are purchased in return for "evaluating" the customer service and other aspects of the store visit.

Like the WFH scheme, the advertisements and websites for mystery shopper scams are designed to look legitimate and blend in with other genuine secret shopper programs. Likewise, recruitment is performed in a similar fashion by using spam email and employment site advertisements.

Scams will often include evaluating a money service business such as Western Union or MoneyGram. Shoppers will receive a counterfeit check, which may be in the amount of several thousand dollars. Shoppers will be instructed to cash the check and use their local Western Union or MoneyGram to send the proceeds to a designated third party account. The shoppers are told to keep a certain amount for themselves and email the fraudster their rating of the service.

Case example: secret shopper scam

A US Navy veteran had difficulty securing full time employment after he completed his military career. While job hunting on the internet he saw an advertisement for a mystery shopper evaluation job and applied. His assignments were easy; he would receive checks via FedEx and then would deposit them into his personal account. He was instructed to purchase Green Dot[10] prepaid cards with the funds. Once he had the Green Dot cards he would call his manager and provide the card numbers and the amount. After the second "assignment" his bank withdrew USD 3,000 to cover the cost of the deposits, which had been counterfeit. The victim reported the incident to his local sheriff's office, but unfortunately there is little that they can do. Read the full article here.

Romance mules

Romance mules usually fall prey to a different type of scam. Romance scams take place online and are deceitful romantic interactions with unsuspecting victims, meant to gain their trust and affections and use that relationship to induce them to commit fraud. Most of the time the victims do not know they are involved in a fraud scheme or criminal act until it is too late.

Romance fraudsters create fake profiles with stolen photographs and false names on high-traffic sites, such as dating websites, social media sites, blog forums and support groups. Upon finding their next victim they will begin contacting them and almost immediately want to communicate privately via e-mail or chat sessions.

The next phase generally lasts from 4 to 6 months, during which the fraudster forms a relationship with the victim. They act as if they are in love with the victim, form bonds and share life stories. The fraudster never lives close to the victim, typically the story is that they live or work abroad, but promise they will visit as soon as they can. Once they are able to get the victim to trust them they begin asking them to receive and transfer money on their behalf.

The fraudster will typically give one or more of the following reasons to explain why they need help:

- Experiencing banking wire issues due to having a foreign account
- Need money in the romance mule's home country to pay for unexpected expenses such as a family member's illness or funeral, employees, or taxes
- Are military personnel stationed overseas who needs assistance accessing their finds due to being in a warzone
- Are inheriting millions and must receive the money in the romance mule's home country
- Need a package or documents to be re-sent to someone in the victim's home country

Once the victim agrees to accept the funds or packages and assist in resending them to others, they have unknowingly become a mule. The packages could contain illegal drugs, weapons or large sums of cash. The deposits will most likely be from stolen or counterfeit checks and transferred funds will be from illicit activities or compromised accounts.

Case example: romance scam

A 61-year-old man in the United Kingdom believed he was corresponding with an affluent businesswoman in her early 60s whom he met on an online dating site. The "woman" claimed she needed to pay some of her employees in the UK, and said they would only trust payments coming from a UK bank account. Once the man agreed, he began receiving large wire transfers into his account and he would prepare and send checks on the "woman's" behalf. The funds were part of a terrorist financing scheme, and the victim was charged with a criminal offence but ultimately found not guilty because he had been duped. Read the article here.

A variation to the romance mule scam is when the mule is being blackmailed to carry out the illegal activities on the fraudsters' behalf. Most of these cases arise because the fraudsters, under the guise of the online love interest, convince the victims to share provocative or sexual photos or videos. The fraudster will then reveal their true nature and threaten to go public with these images or videos if the victim does not assist in their illegal activities.

Warning signs that the person you are talking to is a fraudster:

- **After introductions they want to move the conversation out of the forum or dating website to e-mail, instant messaging or text messaging**
- **They profess love fast and utilize endearing terms and pet names**
- **They claim to live or work abroad, but will be back in your area soon**
- **Their grammar or language skills are slightly off**
- **They want to know all about you and your life, but do not share much about themselves**
- **They ask you to receive money or items and transfer them on their behalf**

Romance scammers prey on people who are vulnerable. Victims who become mules, whether knowingly or unknowingly, are highly traumatized and embarrassed. These scams will often go unreported.

Lottery and inheritance scam mules

These types of scams inform the victims that they have won a lottery or sweepstakes or are to receive an inheritance from a deceased unknown relative. Fraudsters or mule herders initiate these scams in a number of ways; including, but not limited to: e-mail, telephone, letters via USPS mail, faxes, and social media. Once victims respond to the communications the fraudster will then ask the victim for proof of identity. Allegedly this is to facilitate the transfer of payment, when in reality the fraudster is gathering information to potentially steal the victim's identity. Next, the fraudsters will mention legal issues, taxes, insurance, probate fees, or delivery costs.

The way in which fraudsters or mule herders turn these victims into unsuspecting money mules is by offering to assist them in the payment of the "fees" associated with their windfall. The fraudsters inform the victims that the payments are coming from legitimate clients, but in reality the funds usually come from other victims' accounts. The fraudsters or mule herders will wire funds into the victims' account, or on rare occasions use stolen or counterfeit checks. Once the victims have received the funds they are instructed to keep a portion and send the rest to another account. This process effectively turns the victim into a money mule.

Case example: sweepstakes scam

An elderly couple in Raleigh, North Carolina were informed that they had won an international sweepstakes. The fraudsters requested fees in advance and the couple agreed. Once the couple was deep in debt the fraudsters offered to hire them as representatives for the Canadian sweepstakes company. Large sums of cash began to arrive at their home; the couple repackaged and mailed it to other recipients. They also received commissions for their work. The couple's children became suspicious and engaged the assistance of federal authorities. Read the full article here.

In other cases the victims themselves become knowing money mules in order to recoup some of the funds they lost. In these cases the victims fall prey to the advance fee frauds of the inheritance and lottery scams and lose thousands of dollars. The fraudsters or mule herders then work out a deal with the victim to let them earn some of the money back by working as a mule.

Case example: lottery scam

A 74 year old woman living in the US state of Georgia faces felony money laundering charges and theft. The woman fell prey to a Jamaican lottery scam. After she went far into debt, the fraudsters offered her a deal. She could work as a mule for them and they would pay her some of her money back. The victim was so desperate that she agreed, thus moving from victim to perpetrator. Read the full article here.

Emerging trends

The fraud landscape is constantly shifting. The following mule innovations have been identified in recent months and are expected to become more common in the near future.

Visa Waiver Program mules

The Visa Waiver Program (VWP) is an international agreement between, currently, 38 countries.[11] It allows citizens of participating countries to travel to the United States without a visa for stays of 90 days or less, if they meet certain requirements. The VWP permits travel within the US for purposes of tourism and certain business activities.

Figure 3: List of countries participating in the Visa Waiver Program, as of September 2014.

Source: US State Department, Bureau of Consular Affairs

VWP mule activity has been observed in the last 12 to 18 months. The activity to date involves young adults from VWP countries being recruited to travel to the US and open deposit accounts. Upon arrival, the mules will open multiple accounts at various FIs in their true name. The mules provide the bank account information back to their handlers.

The scheme usually involves an EFT deposit to the mule account but it has also been used to deposit tax refund checks obtained through tax refund fraud schemes.

The mules know that they are involved with an illicit scheme; however, they likely don't view what they are doing as illegal. Furthermore, they may believe, or are told, that they are beyond the reach of US law enforcement once they are back in their home country.

Mobile money mules

The concept of the mobile money mule will makes its way into the landscape of fraud and money laundering vectors over the next few years, and will pose a new challenge for FIs.

It is evident that consumers desire the ability to perform bank transactions on their mobile devices, based on a review of data about mobile banking adoption from the Federal Reserve Board:

- Thirty three percent of all mobile phone owners and 51 percent of all smartphone owners have used mobile banking in the past year.
- Twelve percent of mobile phone owners who are not using mobile banking now think that they we will in the next year.
- Uses of mobile banking:
  - Ninety three percent use it to check balances.
  - Fifty seven percent use it to transfer money between accounts.
  - Thirty eight percent have deposited a check in the last year, up from 21 percent in 2013.
- Seventeen percent have used their phone to make a payment in the last year.
- Sixty six percent of the mobile payments were bill payments through an online banking system.

Recent history has shown that cybercriminals proficiently adapt and exploit new technologies and trends. As consumers increasingly adopt mobile banking technology, there will naturally be a demand to do more types of transactions from their mobile device. FIs will strive to provide consumers with the option to do everything via mobile that they can do today in a physical branch location. The customer experience and lower cost of transactions will drive that expansion.

The technology will not likely change the money mule process; however, it may make it easier for criminal syndicates. They will have the ability to establish new accounts through the mobile channel, rather than having the money mules physically go into a branch. This removes the potential detection of suspicious account openings during human interaction.

The ability to open accounts and direct all other transactions through the mobile channel will increase the velocity with which criminal groups may operate. It will also give them more flexibility in the way they communicate and interact with their mules.

One may speculate that increased mobile transaction offerings may eliminate the need for criminal groups and mule herders to recruit money mules. If new accounts could be opened and all other transactions could be executed via mobile; why would a money mule be needed? Accounts could be opened in fake names with fake credentials as they are today, but from the mobile platform. Electronic funds transfers could be initiated out of the FI to a third party from a mobile device. The less human interaction that is needed, then the more flexibility it provides the criminal element.

It is challenging to anticipate the ways in which mobile banking will enable criminal groups to commit fraud and launder money through the use of money mules. What is known, based on past experience, is that criminals will adapt and exploit new technologies and services.

Analysts' comments

The concept of the money mule is not new. They have played an important role in fraud and money laundering for decades. Individuals that receive and transfer money or merchandise to third parties are mules that are needed to help clean, or "launder," stolen money or goods. Some mules know, some suspect, and some have no idea that they are part of an illicit scheme. Professional mules offer their services for hire.

Unknowing mules are typically vulnerable, extremely gullible individuals that are preyed on through romance, lottery and inheritance schemes, often via dating or other social networking sites. Those individuals that know or suspect they are involved in an illicit scheme are often drawn into work-from-home or secret shopper roles by advertisements or spam emails. Many of those individuals are attracted to the seemingly "easy money" that the ads offer. Oftentimes their attraction is out of desperation because an extended period of unemployment or other financial hardship.

In contrast to unknowing mules, the main occupation of the mule herder, professional mule or mule for hire is to receive and transfer money acquired illegally. They are fully aware of the illegal nature of their work. Mule herders are responsible for finding individual's to carry out the illicit activities and are often the ones behind many of the schemes we outlined above. The mules for hire utilize commercially available crimeware to complete their fraud. The J-1 Visa mules who are typically foreign students or summer work program participants that are given fake passports and told to open accounts under an alias for the purposes of transferring money back to their home country or physically smuggling it back.

Money mule transactions represent a serious financial crime threat, particularly money laundering to which FIs may be subject to punitive fines. The FDIC offers the following red flags that may indicate money mule activity:

- A deposit account opened with a minimal deposit soon followed by large EFT deposits.
- Deposit customers who suddenly begin receiving and sending EFTs related to new employment, investments, business opportunities or acquaintances (especially opportunities found on the Internet).
- A newly opened deposit account with an unusual amount of activity, such as account inquiries, or a large dollar amount or high number of incoming EFTs.
- An account that receives incoming EFTs then shortly afterward originates outgoing wire transfers or cash withdrawals approximately eight to ten percent less than the incoming EFTs.
- A foreign exchange student with a J-1 visa and fraudulent passport opening a student account with a high volume of incoming and outgoing EFT activity.

These red flags can be used as part of a comprehensive financial crime strategy. Such a strategy incorporates these red flags and other indicators to help identify the patterns that are indicative of mule activity.

IBM Corporation
Software Group (or appropriate division, or no division)
Route 100
Somers, NY 10589

Produced in the United States of America
September 2014

1 Krebs, Brian http://krebsonsecurity.com/2010/05/fbi-promises-action-against-money-mules/

2 National Crime Prevention Council, The Association of Bank in Singapore, and the Singapore Police Force, joint media release. November 22, 2013

3 Aharoni, I. (2011, April 12). Inside the The Mule Network. Retrieved from Security Week: http://www.securityweek.com/inside-mule-network

4 CryptoLocker is a ransomware trojan that targets computers running Microsoft Windows. When activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers. Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

5 Justice Department press release, retrieved from: http://www.justice.gov/opa/pr/2011/February/11-crm-206.html

6 For more information, see: http://j1visa.state.gov/programs

7 Costa, Daniel. Working Economics, J-1 Summer Work Travel Program Still Poorly Regulated. March 19, 2014 http://www.epi.org/blog/dhs-state-department-j1-summer-work-travel-poorly-regulated/

8 Zetter, Kim. Wired Magazine, U.S. Charges 37 Alleged Mules and Others in Online Bank Fraud Scheme. September 30, 2010 http://www.wired.com/2010/09/zeus-botnet-ring/

9 Matthew DeSantis, C. D. (2011). Understanding and Protecting Yourself Against Money Mule Schemes. Available at: https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf

10 Green Dot (https://www.greendot.com/greendot) is a provider of prepaid Visa or MasterCard debit cards.

11 For details and a list of participating countries, see http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html

12 See http://www.federalreserve.gov/econresdata/mobile-devices/2014-mobile-accessible.htm

Please Recycle