

Stopping Cyber Fraud

LEGAL EDUCATION DEPARTMENT
Attorneys' Title Fund Services, LLC

Unless otherwise noted, all original material is
Copyright © 2018

Attorneys' Title Fund Services, LLC
(800) 336-3863

Please contact The Fund's Education Registrar for information about our programs

EducationRegistrar@thefund.com
(888) 407-7775

All references herein to title insurance policy forms and endorsements are intended to refer to the policy forms and endorsements issued by Fund members as duly appointed title agents of Old Republic National Title Insurance Company.

These materials are for educational use in Fund seminars. They should not be relied on without first considering the law and facts of a matter. Legal documents for others can only be prepared by an attorney after consultation with the client.

Table of Contents

		PDF Page Number
1.	PowerPoint Slides	4
2.	*Start with Security, a Guide for Business,* Fed. Trade Comm., June 2015	25
3.	*Tax Security 101 – Security Summit outlines 'Security Six' basic safeguards for tax professionals' computers and email,* I.R.S., last updated July 17, 2018	42
4.	*E-Mail Account Compromise,* Public Service Announcement Alert No. I-082715b-PSA, Dept. of Justice, Fed. Bur. of Investigation, August 27, 2015	44
5.	*Avoiding Social Engineering and Phishing Attacks,* Security Tip (ST04-014), Nat. Cybersecurity & Comm. Integration Ctr., U.S. Dept. of Homeland Security, last revised January 24, 2017	46
6.	*Phishing Tip Card,* U.S. Dept. of Homeland Security, undated	48
7.	*Choosing and Protecting Passwords,* Security Tip (ST04-0102), Nat. Cybersecurity & Comm. Integration Ctr., U.S. Dept. of Homeland Security, last revised June 22, 2018	50
8.	*Sample Wire Fraud Warnings You Can Use,* American Land Title Association, TitleNews Online Archive, July 27, 2017	53
9.	*Understanding and Protecting Yourself Against Money Mule Schemes,* DeSantis, Dougherty, & McDowell, © 2011 Carnegie Mellon Univ., https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf (last visited September 12, 2018)	54
10.	*Financial Fraud Kill Chain,* Dept. of Justice, Fed. Bur. of Investigation, January 11, 2016	59
11.	*Checklists: Buyer's Fraud, Closer's Fraud, Seller's Fraud,* Attorneys' Title Fund Services, LLC, © 2017	60
12.	*Information Security FAQs,* Attorneys' Title Fund Services, LLC	63
13.	Continuing Education resources	70

© 2018 Attorneys' Title Fund Services, LLC
All Rights Reserved. Duplication Prohibited.
These materials are for educational use in Fund Seminars. They should not be relied on without first considering the law and facts of a matter. Legal documents for others can only be prepared by an attorney after consultation with the client.

Stopping Cyber Fraud

Presented by
The Legal Education Department

The Fund ALWAYS DRIVEN

Accreditation

See course materials handout



70

BEC Real Estate Fraud

The scenario:

- Gain access to email account ("hack")
- Monitor for pending transactions
- Commandeer real email address and create lookalike email addresses ("spoof") for other participants
- Email bogus wire transfer instructions
- Funds wired to criminal-controlled account
- Funds dispersed and trail goes cold



44

3

ALWAYS DRIVEN

Real Estate Market

- **Lucrative** – average wire transfer loss: $200,000
  - Average bank robbery: $7,000
- **Multiple parties** communicating electronically
  - Chain only as strong as weakest link
  - Transaction location irrelevant
- **Fraud tools** easily found online
  - Phishing kits and other technical tools
    - Little technical knowledge needed
  - Attorney, agency, broker, FSBO listings

4

ALWAYS DRIVEN

Perpetrator Tactics



Computer Intrusion

- Malicious attachment or link
  - Activating gives computer access
  - Hacker monitors email traffic
  - Sends email from hacked account

Social Engineering

- Non-technical manipulation
  - Use of knowledge gained from hacked computer and publicly available resources
  - Exploit knowledge of chaos surrounding closing and last minute need to wire funds

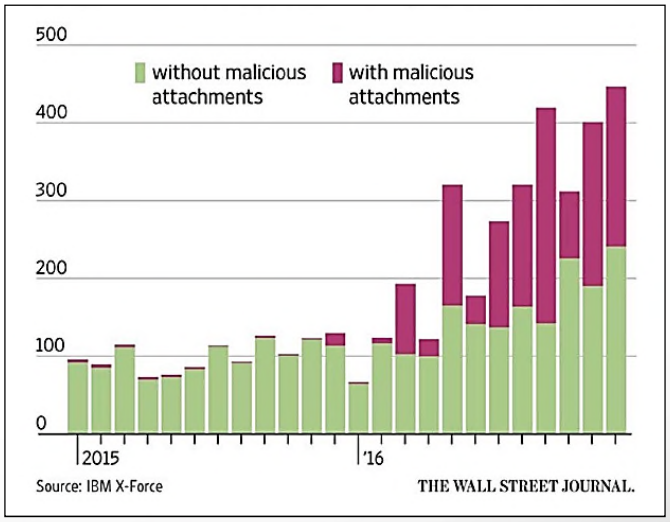
Phases of BEC Fraud

1. Phishing 
2. Hacking (account takeover) 

3. Social engineering 
4. Money muling 

Phishing with Spam

- Mass electronic mailings
- More than half of all email is spam
- Nearly half of all spam is infected



Hook, Line & Sinker



- Staging phishing attacks
  - Phishing kit – easily purchased toolbox
  - Hosting service to launch attack
    - Free, vulnerable, legitimate or illegitimate
    - Google search
    - Use “scanner bots” to locate hosting site
  - Program to send spam
    - Install emailer program – typically on hacked server
    - “Spam bots”
    - Underground spamming service

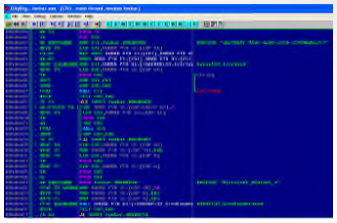
48

Hook, Line & Sinker



- Staging phishing attacks
  - Craft phishing email "lure"
    - Templates found online
    - Copy legitimate email and replace links
  - Obtain email address list
    - Purchase online
    - Use "bots" to crawl public websites
    - Download from compromised webmail accounts
    - Malware on infected PCs
  - Launch attack and wait for a bite!
    - More than 90% of cybercrime begins with phishing

Hook, Line & Sinker



- Launch and wait
  - Broker, agency, title firm targets
  - Multiple email accounts receive malignant spam
  - Victim's "click" silently downloads malware
- Malware responds
  - Sets up new default rules for account
    - Auto-forwards to fraudster's server any email containing keywords (e.g., purchase, escrow, contract, down payment, etc.)
    - Auto-delete replies to hacker initiated email
  - "Mines" account for NPI, etc.

Account Takeover





Computer Intrusion

Malware (malicious software)

- Display unwanted advertising
- Disrupt computer operations
- Gather sensitive information
- **Gain access to private computer systems**

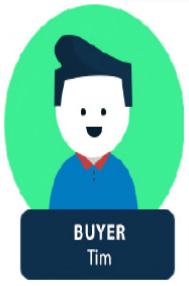


Bogus Email to Agent









OCTOBER 17, 2016

9:02 AM



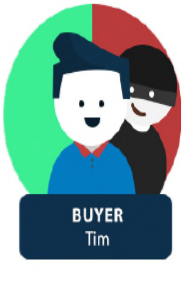


Spoofed Buyer Email









OCTOBER 17, 2016

9:02 AM





9:09 AM





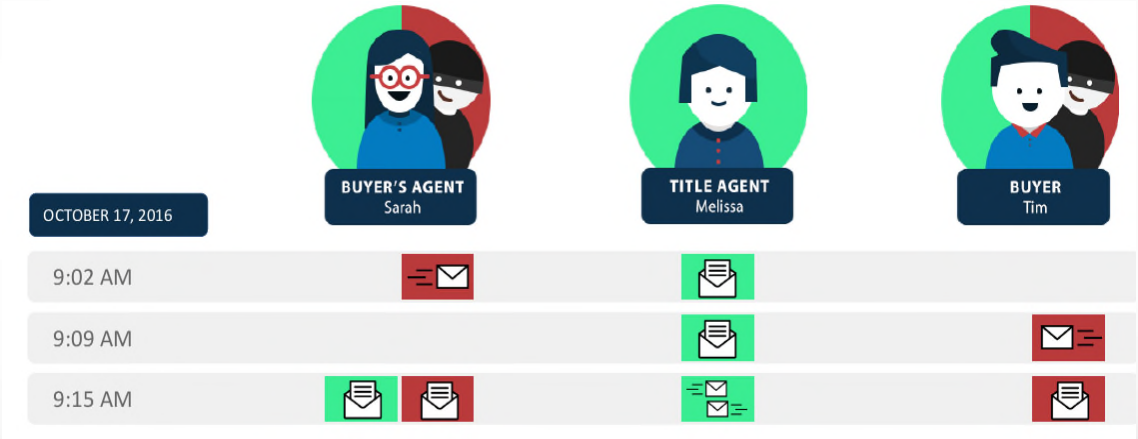
Spoofed Email

Tim: tsmith@gmail.com

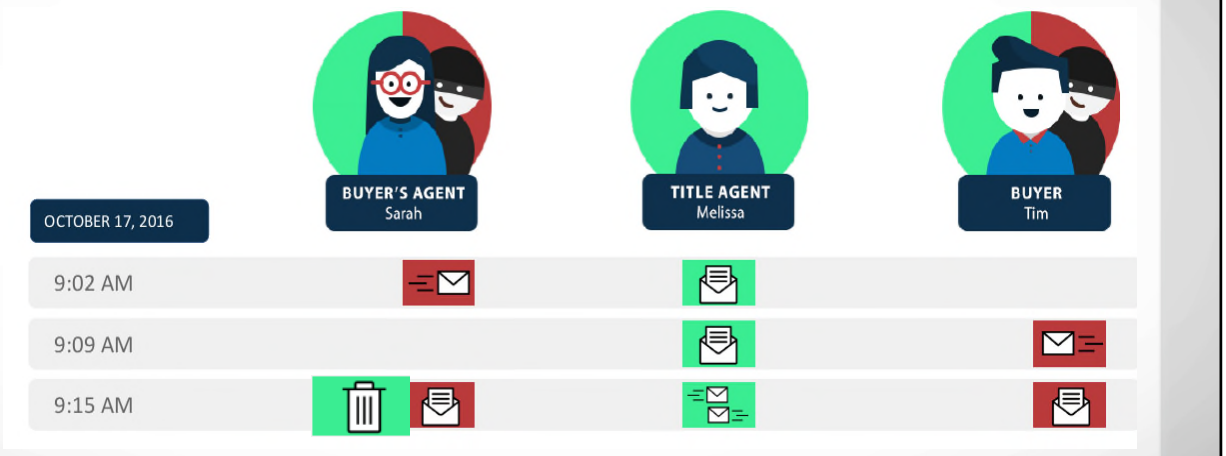
Fraudulent Tim:
tsmith1@gmail.com



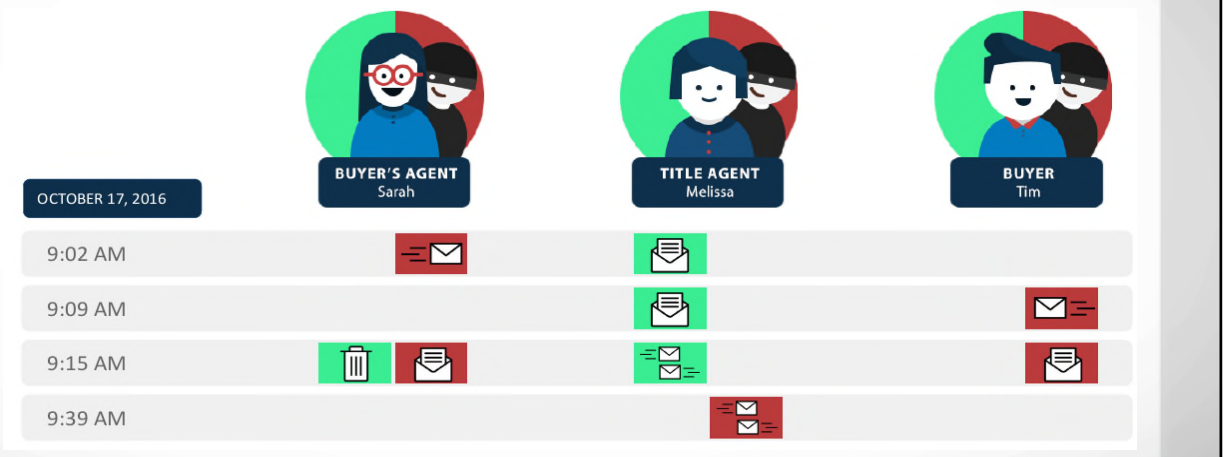
Agent Emails "Parties"



Auto-deleted



Spoofed Agent Email



Spoofed Email

Melissa: mdombrowski@suntitleagency.com

Fraudulent Melissa:
mdombrowski@suntitleagency.com



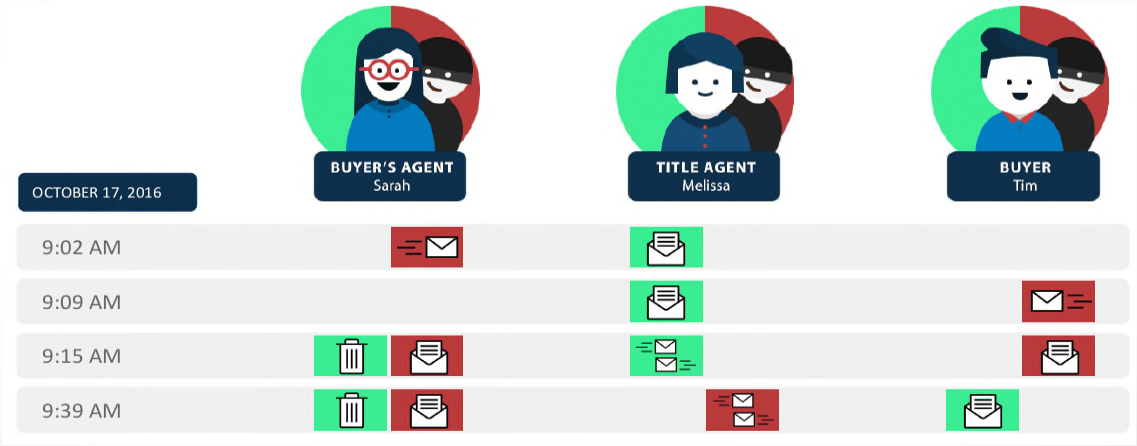
Spoofed Email

Melissa:
mdombrowski@suntitleagency.com

Fraudulent Melissa:
mdombrowski@suntitIeagency.com

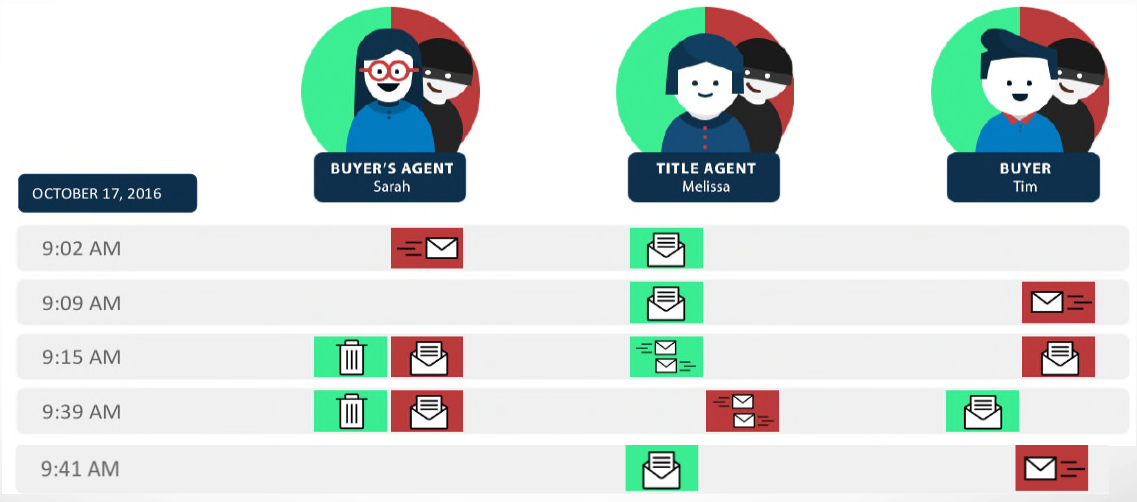


Auto-delete / Buyer Opens



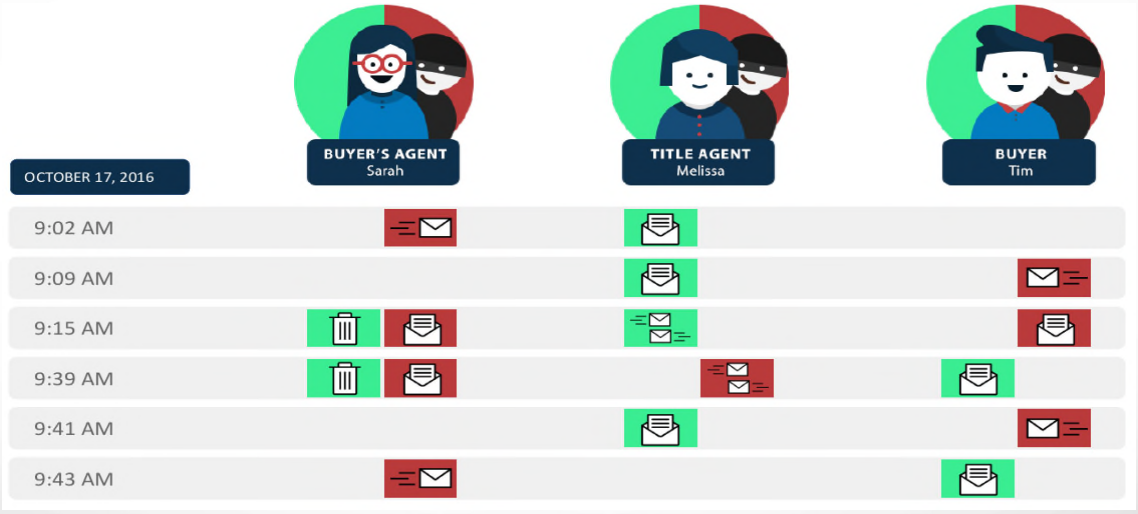
Spoofed Buyer Email





Bogus Email to Buyer





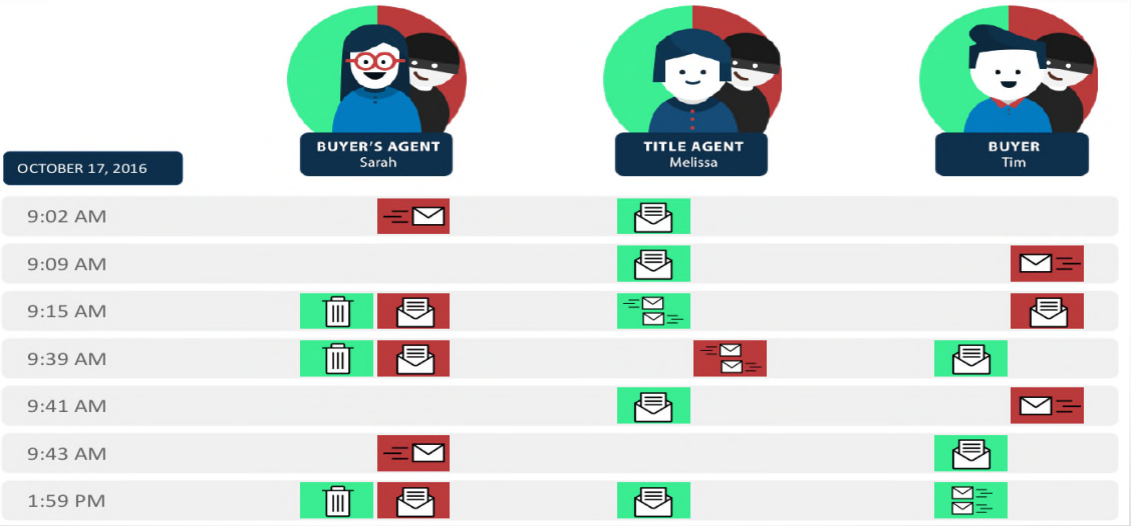
Buyer Initiates Transfer





Buyer Confirms Wire





Money Muling



- Bridges the gap between victim and attacker
  - Shields identity of cybercriminal
- Initial recipients of wire transfers
- Funds disbursed to money mule's recruiter
  - ATM withdrawals
  - Wire transfers
- Recruiters forward $$$ to cybercriminals
  - Foreign wire transfers
  - Moneygrams
  - Cryptocurrency

Recruitment



- Face-to-face
  - Sad story
  - Golden opportunity
  - Exchange ATM card and pin code
- Online
  - Job/romance scam
  - Respond to C/V posting
- Phone
  - Street corner signs (e.g., work from home; foreclosure relief)

Money Mule



- Surrender control of account to recruiter
  - ATM and Pin for cash withdrawals
  - Typically for identity theft financial fraud
- Agree to use account as directed by recruiter
  - Keep a small percentage as payment
  - Forward balance by foreign wire transfer
  - Often duped into believing funds are legitimate (e.g., recruiter unable to use regular financial channels)

Money Mule



- Greedy
  - Lots of money for little work
- Gullible
  - Friend in need; foreign relatives sending money; romantic relationship request
- Financial strain
  - Looking for work; short term goals
- Penalties
  - Petit theft
  - Judgment proof

29

ALWAYS DRIVEN

When Fraud Occurs…



- Contact sending bank immediately
  - Wire reversal
  - Contact recipient bank
  - Financial Fraud Kill Chain (FFKC) process
- Contact local FBI field office – rapid response protocol
- Visit www.ic3.gov to file a complaint

59

30

ALWAYS DRIVEN

www.ics.gov



www.ics.gov



www.ics.gov

Note: Fields marked with * are required.

Victim Information

* **Name:**
Business Name:
Age: Please select one...
* **Address:**
Address (continued):
Suite/Apt./Mail Stop:
* **City:**
County:
* **Country:** Please Select One...
State: [None]
* **Zip Code/Route:**
* **Phone Number:** numbers only (1112223333)
* **Email Address:** jdoe@email.com
Business IT POC, if applicable: Name, Email, Phone number, etc.
Other Business POC, if applicable: Name, Email, Phone number, etc.

Information About The Subject(s) Who Victimized You

Financial Transaction(s)

Description of Incident

Other Information

Who Filed the Complaint

Privacy Act Statement

Digital Signature

Submit Complaint

When Fraud Occurs…



- Do not destroy or delete records related to the transaction
- Do not attempt to communicate with the perpetrators
- Do notify your title underwriter and (if applicable) your E&O or Cyber-Fraud Carrier

Cyber Fraud Defense

- Do not use **free email accounts** for business purposes (e.g., AOL, Gmail, Yahoo, etc.)
  - Easier to hack
- Create contact information log at the outset of transaction with all parties' phone numbers



35

ALWAYS DRIVEN

Cyber Fraud Defense

- Have parties sign funds transfer agreement at the outset of transaction
- If procedure changes confirm by calling phone number in the log
- Beware of pressure to quickly change payment arrangements. Slow down if necessary; and <u>stay in control of the transaction</u>



Buyer's Fraud
CHECKLIST

Begin the Transaction Securely

- Establish at least one trusted phone number for your real estate agent and settlement agent soon after your sales contract is signed.
- **Real estate agents** - phone numbers are often on the contract or listing agreement. You can also trust the brokerage's website or telephone directory.
- **Settlement agent** - you may get a letter or some other "opening" correspondence from the settlement agent. If you visit in person, pick up a business card. You can also trust the settlement agent's website or telephone directory. If your settlement agent is an attorney, their information can be obtained at www.flabar.org.
- Use a more "secure" email address for any correspondence about the transaction. Consider using your work email address because there are generally more firewalls and security protocols. Avoid free, internet-based accounts like Yahoo and Gmail.
- Do not send any personal or private information via email, including your social security number and identification documents. If you wouldn't share the information on Facebook, don't put it in your email!
- Verify any changes to the settlement agent's contact information or wiring instructions either in person or via the trusted phone number given at the beginning of the transaction.

60

36

ALWAYS DRIVEN

Two Factor Authentication



Phone call to verify legitimacy of every communication directing transfer of funds

- Parties acknowledge protocol at start of transaction
- Verification phone number must not come from the un-authenticated communication
- Parties acknowledge funds will not be directed or re-directed on un-authenticated communications
- After funds are wired, confirm receipt by calling the recipient's number in the log

37

Cyber Fraud Self Defense

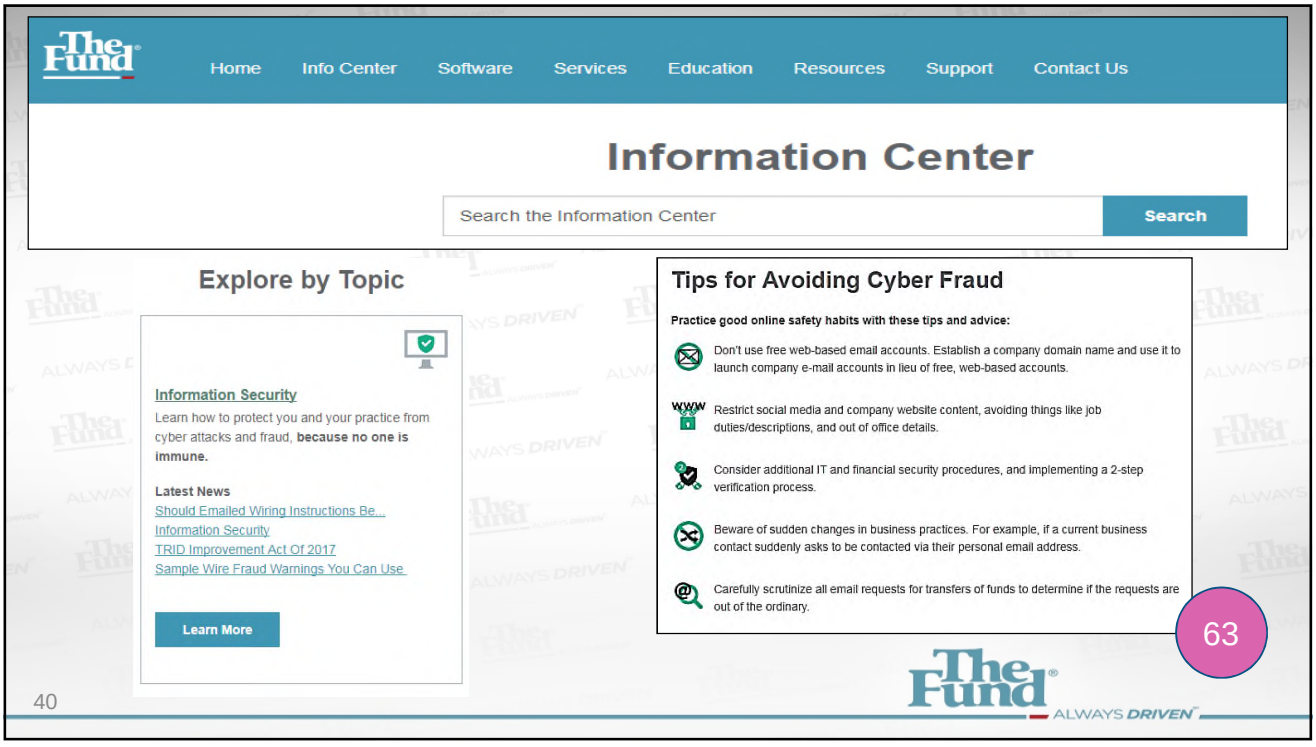
- Do not "click" on suspicious or unknown email attachments or links
- Use strong passwords and change them throughout the office frequently
- Don't publicize when managers are travelling out of town, especially on social media sites
- Train staff on protocol
- Keep anti-virus software up to date



38

Takeaways

- Successful hacks typically reside on computer 100 days before detection
- Every transaction is targeted (not just real estate)
- Every wire transfer is potentially divertible
- Verbal confirmation includes reading the wire instructions (just like confirming legal descriptions)
- Best practices will not stop the problem
  - Lessen likelihood of successful attack
  - Mitigate damages if sued



THANK YOU!

Comments & Questions

RRohan@TheFund.com

The Fund® ALWAYS DRIVEN™

START WITH SECURITY

A GUIDE FOR BUSINESS

LESSONS LEARNED FROM FTC CASES

FEDERAL TRADE COMMISSION

START WITH SECURITY

1. **Start with security.**
2. **Control access to data sensibly.**
3. **Require secure passwords and authentication.**
4. **Store sensitive personal information securely and protect it during transmission.**
5. **Segment your network and monitor who's trying to get in and out.**
6. **Secure remote access to your network.**
7. **Apply sound security practices when developing new products.**
8. **Make sure your service providers implement reasonable security measures.**
9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**
10. **Secure paper, physical media, and devices.**

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant. As the Federal Trade Commission outlined in *Protecting Personal Information: A Guide for Business,* you should know what personal information you have in your files and on your computers, and keep only what you need for your business. You should protect the information that you keep, and properly dispose of what you no longer need. And, of course, you should create a plan to respond to security incidents.

In addition to *Protecting Personal Information*, the FTC has resources to help you think through how those principles apply to your business. There's an online tutorial to help train your employees; publications to address particular data security challenges; and news releases, blog posts, and guidance to help you identify – and possibly prevent – pitfalls.

There's another source of information about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far. These are settlements – no findings have been made by a court – and the specifics of the orders apply just to those companies, of course. But learning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps. Distilling the facts of those cases down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.

1 Start with security.

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Business executives often ask how to manage confidential information. Experts agree on the key first step: Start with security. Factor it into the decisionmaking in every department of your business – personnel, sales, accounting, information technology, etc. Collecting and maintaining information "just because" is no longer a sound business strategy. Savvy companies think through the implication of their data decisions. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road. Of course, all of those decisions will depend on the nature of your business. Lessons from FTC cases illustrate the benefits of building security in from the start by going lean and mean in your data collection, retention, and use policies.

Don't collect personal information you don't need.

Here's a foundational principle to inform your initial decision-making: No one can steal what you don't have. When does your company ask people for sensitive information? Perhaps when they're registering online or setting up a new account. When was the last time you looked at that process to make sure you really need everything you ask for? That's the lesson to learn from a number of FTC cases. For example, the FTC's complaint against ***RockYou*** charged that the company collected lots of information during the site registration process, including the user's email address and email password. By collecting email passwords – not something the business needed – and then storing them in clear text, the FTC said the company created an unnecessary risk to people's email accounts. The business could have avoided that risk simply by not collecting sensitive information in the first place.

Hold on to information only as long as you have a legitimate business need.

Sometimes it's necessary to collect personal data as part of a transaction. But once the deal is done, it may be unwise to keep it. In the FTC's ***BJ's Wholesale Club*** case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company's security practices, hackers stole the account data and used it to make counterfeit credit and debit cards. The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need for it.

Don't use personal information when it's not necessary.

You wouldn't juggle with a Ming vase. Nor should businesses use personal information in contexts that create unnecessary risks. In the ***Accretive*** case, the FTC alleged that the company used real people's personal information in employee training sessions, and then failed to remove the information from employees' computers after the sessions were over. Similarly, in ***foru International***, the FTC charged that the company gave access to sensitive consumer data to service providers who were developing applications for the company. In both cases, the risk could have been avoided by using fictitious information for training or development purposes.

2 Control access to data sensibly.

Once you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. You'll want to keep it from the prying eyes of outsiders, of course, but what about your own employees? Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a "need to know" basis. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet. When thinking about how to control access to sensitive information in your possession, consider these lessons from FTC cases.

Restrict access to sensitive data.

If employees don't have to use personal information as part of their job, there's no need for them to have access to it. For example, in ***Goal Financial***, the FTC alleged that the company failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. The company could have prevented that misstep by implementing proper controls and ensuring that only authorized employees with a business need had access to people's personal information.

Limit administrative access.

Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job. In its action against ***Twitter***, for example, the FTC alleged that the company granted almost all of its employees administrative control over Twitter's system, including the ability to reset user account passwords, view users' nonpublic tweets, and send tweets on users' behalf. According to the complaint, by providing administrative access to just about everybody in-house, Twitter increased the risk that a compromise of any of its employees' credentials could result in a serious breach. How could the company have reduced that risk? By ensuring that employees' access to the system's administrative controls was tailored to their job needs.

3 Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password "hygiene" – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are tips to take from FTC cases.

Insist on complex and unique passwords.

"Passwords" like 121212 or qwerty aren't much better than no passwords at all. That's why it's wise to give some thought to the password standards you implement. In the ***Twitter*** case, for example, the company let employees use common dictionary words as administrative passwords, as well as passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools, or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system – for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts.

Store passwords securely.

Don't make it easy for interlopers to access passwords. In ***Guidance Software***, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker access customer credit card information on the network. Similarly, in ***Reed Elsevier***, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers. In ***Twitter***, too, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts. In each of those cases, the risks could have been reduced if the companies had policies and procedures in place to store credentials securely. Businesses also may want to consider other protections – two-factor authentication, for example – that can help protect against password compromises.

Guard against brute force attacks.

Remember that adage about an infinite number of monkeys at an infinite number of typewriters? Hackers use automated programs that perform a similar function. These brute force attacks work by typing endless combinations of characters until hackers luck into someone's password. In the ***Lookout Services***, ***Twitter***, and ***Reed Elsevier*** cases, the FTC alleged that the businesses didn't suspend or disable user credentials after a certain number of unsuccessful login attempts. By not adequately restricting the number of tries, the companies placed their networks at risk. Implementing a policy to suspend or disable accounts after repeated login attempts would have helped to eliminate that risk.

Protect against authentication bypass.

Locking the front door doesn't offer much protection if the back door is left open. In ***Lookout Services***, the FTC charged that the company failed to adequately test its web application for widely-known security flaws, including one called "predictable resource location." As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

4 Store sensitive personal information securely and protect it during transmission.

For many companies, storing sensitive data is a business necessity. And even if you take appropriate steps to secure your network, sometimes you have to send that data elsewhere. Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. But regardless of the method, it's only as good as the personnel who implement it. Make sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation. With that in mind, here are a few lessons from FTC cases to consider when securing sensitive information during storage and transmission.

Keep sensitive information secure throughout its lifecycle.

Data doesn't stay in one place. That's why it's important to consider security at all stages, if transmitting information is a necessity for your business. In ***Superior Mortgage Corporation***, for example, the FTC alleged that the company used SSL encryption to secure the transmission of sensitive personal information between the customer's web browser and the business's website server. But once the information reached the server, the company's service provider decrypted it and emailed it in clear, readable text to the company's headquarters and branch offices. That risk could have been prevented by ensuring the data was secure throughout its lifecycle, and not just during the initial transmission.

Use industry-tested and accepted methods.

When considering what technical standards to follow, keep in mind that experts already may have developed effective standards that can apply to your business. Savvy companies don't start from scratch when it isn't necessary. Instead, they take advantage of that collected wisdom. The ***ValueClick*** case illustrates that principle. According to the FTC, the company stored sensitive customer information collected through its e-commerce sites in a database that used a non-standard, proprietary form of encryption. Unlike widely-accepted encryption algorithms that are extensively tested, the complaint charged that ValueClick's method used a simple alphabetic substitution system subject to significant vulnerabilities. The company could have avoided those weaknesses by using tried-and-true industry-tested and accepted methods for securing data.

Ensure proper configuration.

Encryption – even strong methods – won't protect your users if you don't configure it properly. That's one message businesses can take from the FTC's actions against ***Fandango*** and ***Credit Karma***. In those cases, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned off a critical process known as SSL certificate validation without implementing other compensating security measures. That made the apps vulnerable to man-in-the-middle attacks, which could allow hackers to decrypt sensitive information the apps transmitted. Those risks could have been prevented if the companies' implementations of SSL had been properly configured.

5 Segment your network and monitor who's trying to get in and out.

When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet. Another useful safeguard: intrusion detection and prevention tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Segment your network.

Not every computer in your system needs to be able to communicate with every other one. You can help protect particularly sensitive data by housing it in a separate secure place on your network. That's a lesson from the ***DSW*** case. The FTC alleged that the company didn't sufficiently limit computers from one in-store network from connecting to computers on other in-store and corporate networks. As a result, hackers could use one in-store network to connect to, and access personal information on, other in-store and corporate networks. The company could have reduced that risk by sufficiently segmenting its network.

Monitor activity on your network.

"Who's that knocking on my door?" That's what an effective intrusion detection tool asks when it detects unauthorized activity on your network. In the ***Dave & Buster's*** case, the FTC alleged that the company didn't use an intrusion detection system and didn't monitor system logs for suspicious activity. The FTC says something similar happened in ***Cardsystem Solutions***. The business didn't use sufficient measures to detect unauthorized access to its network. Hackers exploited weaknesses, installing programs on the company's network that collected stored sensitive data and sent it outside the network every four days. In each of these cases, the businesses could have reduced the risk of a data compromise or its breadth by using tools to monitor activity on their networks.

6 Secure remote access to your network.

Business doesn't just happen in the office. While a mobile workforce can increase productivity, it also can pose new security challenges. If you give employees, clients, or service providers remote access to your network, have you taken steps to secure those access points? FTC cases suggest some factors to consider when developing your remote access policies.

Ensure endpoint security.

Just as a chain is only as strong as its weakest link, your network security is only as strong as the weakest security on a computer with remote access to it. That's the message of FTC cases in which companies failed to ensure that computers with remote access to their networks had appropriate endpoint security. For example, in ***Premier Capital Lending***, the company allegedly activated a remote login account for a business client to obtain consumer reports, without first assessing the business's security. When hackers accessed the client's system, they stole its remote login credentials and used them to grab consumers' personal information. According to the complaint in ***Settlement One***, the business allowed clients that didn't have basic security measures, like firewalls and updated antivirus software, to access consumer reports through its online portal. And in ***Lifelock***, the FTC charged that the company failed to install antivirus programs on the computers that employees used to remotely access its network. These businesses could have reduced those risks by securing computers that had remote access to their networks.

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should have an all-access, backstage pass. That's why it's wise to limit access to what's needed to get the job done. In the ***Dave & Buster's*** case, for example, the FTC charged that the company failed to adequately restrict third-party access to its network. By exploiting security weaknesses in the third-party company's system, an intruder allegedly connected to the network numerous times and intercepted personal information. What could the company have done to reduce that risk? It could have placed limits on third-party access to its network – for example, by restricting connections to specified IP addresses or granting temporary, limited access.

7 Apply sound security practices when developing new products.

So you have a great new app or innovative software on the drawing board. Early in the development process, think through how customers will likely use the product. If they'll be storing or sending sensitive information, is your product up to the task of handling that data securely? Before going to market, consider the lessons from FTC cases involving product development, design, testing, and roll-out.

Train your engineers in secure coding.

Have you explained to your developers the need to keep security at the forefront? In cases like ***MTS***, ***HTC America***, and ***TRENDnet***, the FTC alleged that the companies failed to train their employees in secure coding practices. The upshot: questionable design decisions, including the introduction of vulnerabilities into the software. For example, according to the complaint in ***HTC America***, the company failed to implement readily available secure communications mechanisms in the logging applications it pre-installed on its mobile devices. As a result, malicious third-party apps could communicate with the logging applications, placing consumers' text messages, location data, and other sensitive information at risk. The company could have reduced the risk of vulnerabilities like that by adequately training its engineers in secure coding practices.

Follow platform guidelines for security.

When it comes to security, there may not be a need to reinvent the wheel. Sometimes the wisest course is to listen to the experts. In actions against ***HTC America***, ***Fandango***, and ***Credit Karma***, the FTC alleged that the companies failed to follow explicit platform guidelines about secure development practices. For example, Fandango and Credit Karma turned off a critical process known as SSL certificate validation in their mobile apps, leaving the sensitive information consumers transmitted through those apps open to interception through man-in-the-middle attacks. The companies could have prevented this vulnerability by following the iOS and Android guidelines for developers, which explicitly warn against turning off SSL certificate validation.

Verify that privacy and security features work.

If your software offers a privacy or security feature, verify that the feature works as advertised. In ***TRENDnet***, for example, the FTC charged that the company failed to test that an option to make a consumer's camera feed private would, in fact, restrict access to that feed. As a result, hundreds of "private" camera feeds were publicly available. Similarly, in ***Snapchat***, the company advertised that messages would "disappear forever," but the FTC says it failed to ensure the accuracy of that claim. Among other things, the app saved video files to a location outside of the app's sandbox, making it easy to recover the video files with common file browsing tools. The lesson for other companies: When offering privacy and security features, ensure that your product lives up to your advertising claims.

Test for common vulnerabilities.

There is no way to anticipate every threat, but some vulnerabilities are commonly known and reasonably foreseeable. In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities. For example, in the ***Guess?*** case, the FTC alleged that the business failed to assess whether its web application was vulnerable to Structured Query Language (SQL) injection attacks. As a result, hackers were able to use SQL attacks to gain access to databases with consumers' credit card information. That's a risk that could have been avoided by testing for commonly-known vulnerabilities, like those identified by the Open Web Application Security Project (OWASP).

8 Make sure your service providers implement reasonable security measures.

When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to develop apps. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they're meeting your requirements. FTC cases offer advice on what to consider when hiring and overseeing service providers.

Put it in writing.

Insist that appropriate security standards are part of your contracts. In ***GMR Transcription***, for example, the FTC alleged that the company hired service providers to transcribe sensitive audio files, but failed to require the service provider to take reasonable security measures. As a result, the files – many containing highly confidential health-related information – were widely exposed on the internet. For starters, the business could have included contract provisions that required service providers to adopt reasonable security precautions – for example, encryption.

Verify compliance.

Security can't be a "take our word for it" thing. Including security expectations in contracts with service providers is an important first step, but it's also important to build oversight into the process. The ***Upromise*** case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed that the toolbar, which collected consumers' browsing information to provide personalized offers, would use a filter to "remove any personally identifiable information" before transmission. But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise's privacy and security policies and the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information – including financial account numbers and security codes from secure web pages – and transmitted it in clear text. How could the company have reduced that risk? By asking questions and following up with the service provider during the development process.

9 Put procedures in place to keep your security current and address vulnerabilities that may arise.

Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to keep your guard up. If you use third-party software on your networks, or you include third-party software libraries in your applications, apply updates as they're issued. If you develop your own software, how will people let you know if they spot a vulnerability, and how will you make things right? FTC cases offer points to consider in thinking through vulnerability management.

Update and patch third-party software.

Outdated software undermines security. The solution is to update it regularly and implement third-party patches. In the ***TJX Companies*** case, for example, the FTC alleged that the company didn't update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business's defenses. Depending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.

Heed credible security warnings and move quickly to fix them.

When vulnerabilities come to your attention, listen carefully and then get a move on. In the ***HTC America*** case, the FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant that the vulnerabilities found their way onto even more devices across multiple operating system versions. Sometimes, companies receive security alerts, but they get lost in the shuffle. In ***Fandango***, for example, the company relied on its general customer service system to respond to warnings about security risks. According to the complaint, when a researcher contacted the business about a vulnerability, the system incorrectly categorized the report as a password reset request, sent an automated response, and marked the message as "resolved" without flagging it for further review. As a result, Fandango didn't learn about the vulnerability until FTC staff contacted the company. The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security@yourcompany.com) for receiving reports and flagging them for your security staff.

10 Secure paper, physical media, and devices.

Network security is a critical consideration, but many of the same lessons apply to paperwork and physical media like hard drives, laptops, flash drives, and disks. FTC cases offer some things to consider when evaluating physical security at your business.

Securely store sensitive files.

If it's necessary to retain important paperwork, take steps to keep it secure. In the ***Gregory Navone*** case, the FTC alleged that the defendant maintained sensitive consumer information, collected by his former businesses, in boxes in his garage. In ***Lifelock***, the complaint charged that the company left faxed documents that included consumers' personal information in an open and easily accessible area. In each case, the business could have reduced the risk to their customers by implementing policies to store documents securely.

Protect devices that process personal information.

Securing information stored on your network won't protect your customers if the data has already been stolen through the device that collects it. In the 2007 ***Dollar Tree*** investigation, FTC staff said that the business's PIN entry devices were vulnerable to tampering and theft. As a result, unauthorized persons could capture consumer's payment card data, including the magnetic stripe data and PIN, through an attack known as "PED skimming." Given the novelty of this type of attack at the time, and a number of other factors, staff closed the investigation. However, attacks targeting point-of-sale devices are now common and well-known, and businesses should take reasonable steps to protect such devices from compromise.

Keep safety standards in place when data is en route.

Savvy businesses understand the importance of securing sensitive information when it's outside the office. In ***Accretive***, for example, the FTC alleged that an employee left a laptop containing more than 600 files, with 20 million pieces of information related to 23,000 patients, in the locked passenger compartment of a car, which was then stolen. The ***CBR Systems*** case concerned alleged unencrypted backup tapes, a laptop, and an external hard drive – all of which contained sensitive information – that were lifted from an employee's car. In each case, the business could have reduced the risk to consumers' personal information by implementing reasonable security policies when data is en route. For example, when sending files, drives, disks, etc., use a mailing method that lets you track where the package is. Limit the instances when employees need to be out and about with sensitive data in their possession. But when there's a legitimate business need to travel with confidential information, employees should keep it out of sight and under lock and key whenever possible.

Dispose of sensitive data securely.

Paperwork or equipment you no longer need may look like trash, but it's treasure to identity thieves if it includes personal information about consumers or employees. For example, according to the FTC complaints in ***Rite Aid*** and ***CVS Caremark***, the companies tossed sensitive personal information – like prescriptions – in dumpsters. In ***Goal Financial***, the FTC alleged that an employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text. The companies could have prevented the risk to consumers' personal information by shredding, burning, or pulverizing documents to make them unreadable and by using available technology to wipe devices that aren't in use.

Looking for more information?

The FTC's Business Center (**business.ftc.gov**) has a Data Security section with an up-to-date listing of relevant cases and other free resources.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Visit the Business Center at **business.ftc.gov**.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman.**



Federal Trade Commission
business.ftc.gov
June 2015

IRS

Tax Security 101 – Security Summit outlines 'Security Six' basic safeguards for tax professionals' computers and email

IR-2018-150, July 17, 2018

WASHINGTON – The Internal Revenue Service and the Security Summit partners outlined critical steps for tax professionals to protect their computers and email as well as safeguarding sensitive taxpayer data.

The "Security Six" protections fall into several major security categories. The Security Summit partnership urges tax professionals across the nation to avoiding overlooking these basic security details as identity thieves increasingly target practitioners in search of valuable taxpayer data.

There is a dizzying array of cyber threats that confront tax professionals and many others. It's not easy to keep up with all the viruses, worms, Trojan horses, bots – or even the terminology. That's why it's essential that all tax professionals deploy strong security software that will do the job for you.

The Internal Revenue Service, state tax agencies and the private-sector tax industry – known as the Security Summit partners – today are trying to help tax professionals decipher the confusing world of security software that is key to safeguarding taxpayer data stored on practitioner's computer networks.

This is the second in a series called "Protect Your Clients; Protect Yourself: Tax Security 101." The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

Although the Security Summit is making progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices is on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

Here are the "Security Six," the must-have areas to secure taxpayer data on computers. All tax professionals, whether part of a large firm or a one-person shop, must enact security safeguards. Many of these steps are a good idea not just for tax professionals but for any taxpayer or small business:

Antivirus software

Although details may vary between packages, anti-virus software scans files or computer's memory for certain patterns that may indicate the presence of malicious software (i.e., malware). Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware. Anti-virus vendors find new and updated malware daily, so it is important that users have the latest updates installed on their computer, according to the U.S. Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security.

Once users have installed an anti-virus package, they should scan their entire computer periodically:

- Automatic scans – Most anti-virus software can be configured to automatically scan specific files or directories in real time and prompt users at set intervals to perform complete scans.
- Manual scans – If the anti-virus software does not automatically scan new files, users should manually scan files and media received from an outside source before opening them. This process includes:
    - Saving and scanning email attachments or web downloads rather than opening them directly from the source.
    - Scanning portable media, including CDs and DVDs, for malware before opening files.

Sometimes the software will produce a dialog box with an alert that it has found malware and ask whether users want it to "clean" the file (to remove the malware). In other cases, the software may attempt to remove the malware without asking first. When selecting an anti-virus package, learn about its features so you know what to expect. Keep security software set to automatically receive the latest updates so that it is always current.

A reminder about spyware: Strong security software should protect against spyware. But remember, never click links within pop-up windows, never download "free" software from a pop-up, never follow email links that offer anti-spyware software. The links and pop-ups may be installing the spyware they claim to be eliminating.

A reminder about phishing: A strong security package also should contain anti-phishing capabilities, but an email provider and browser provider also should include anti-phishing protections. Never open an email from a suspicious source, click on a link in a suspicious email or open an attachment – or else you could be a victim of a phishing attack.

Firewalls

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network. Firewalls can be configured to block data from certain locations or applications while allowing relevant and necessary data through, according to US-CERT.

Firewalls may be broadly categorized as hardware or software. While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use.

- **Hardware** – Typically called network firewalls, these external devices are positioned between a computer and the internet (or other network connection). Many vendors and some internet service providers (ISPs) offer integrated small office / home office (SOHO) routers that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them. The advantage of hardware-based firewalls is that they are separate devices running their own operating systems, so they provide an additional line of defense against attacks when compared to system or host-level protections.

- **Software –** Most operating systems include a built-in firewall feature that should be enabled for added protection even if using an external firewall. Firewall software can also be obtained as separate software from a local computer store, software vendor or ISP. If downloading firewall software from the internet, make sure it is from a reputable source (i.e., an established software vendor or service provider) and offered via a secure site.

While properly configured firewalls may be effective at blocking some attacks, don't be lulled into a false sense of security. Firewalls do not guarantee that a computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (malware), and may not protect the device if the user accidentally installs malware. However, using a firewall in conjunction with other protective measures (such as anti-virus software and safe computing practices) will strengthen resistance to attacks.

The Security Summit reminds tax pros that anti-virus software and firewalls cannot protect data if computer users fall for email phishing scams and divulge sensitive data, such as usernames and passwords. The user, not the software, is the first-line of defense in protecting taxpayer data.

Two-factor authentication

Many email providers now offer customers two-factor authentication protections to access email accounts. Tax professionals should always use this option to prevent their accounts from being taken over by cybercriminals and putting their clients and colleagues at risk.

Two-factor authentication helps by adding an extra layer of protection. Often two-factor authentication means the returning user must enter credentials (username and password) plus another step such as entering a security code sent via text to a mobile phone. The idea is a thief may be able to steal the username and password but it's highly unlikely they also would have a user's mobile phone to receive a security code and complete the process.

The use of two-factor authentication and even three-factor authentication is on the rise, and tax preparers should always opt for a multi-factor authentication protection when it is offered, whether on an email account or tax software account or any password-protected product. IRS Secure Access, which protects IRS.gov tools including e-Services, is an example of two-factor authentication. Check email account settings to see if the email provider offers two-factor protections.

Backup software/services

Critical files on computers should routinely be backed up to external sources. This means a copy of the file is made and stored either online as part of a cloud storage service or similar product. Or, a copy of the file is made to an external disk, such as an external hard drive that now comes with multiple terabytes of storage capacity. Tax professionals should ensure that taxpayer data that is backed up also is encrypted.

Drive encryption

Given the sensitive client data maintained on tax practitioners' computers, users should consider drive encryption software for full-disk encryption. Drive encryption, or disk encryption, transforms data on the computer into unreadable files for the unauthorized person accessing the computer. Drive encryption may come as a stand-alone security software product. It may also include encryption for removable media, such as a thumb drive and its data.

Data security plan

The Security Summit also reminds tax professionals of several other important steps. All professional tax return preparers must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. Tax professionals also can get help with security recommendations and creating a data security plan by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security: the Fundamentals by the National Institute of Standards and Technology.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation data theft information available on IRS.gov. Also, tax professionals should stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts and Social Media.

Page Last Reviewed or Updated: 17-Jul-2018

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

August 27, 2015

Alert Number
I-082715b-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

E-MAIL ACCOUNT COMPROMISE

E-mail Account Compromise (EAC) is a sophisticated scam that targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms.

The EAC scam is very similar to the Business E-mail Compromise (BEC) scam, except that it targets individuals rather than businesses.[1]

In EAC scams, criminal actors use social engineering or computer intrusion techniques to compromise the e-mail accounts of unsuspecting victims. In many cases, a criminal actor first gains access to a victim's legitimate e-mail address for reconnaissance purposes. The criminal actor then creates a spoofed e-mail account that closely resembles the legitimate account, but is slightly altered by adding, changing, or deleting a character. The spoofed e-mail address is designed to mimic the legitimate e-mail in a way that is not readily apparent to the targeted individual. The criminal actor then uses either the victim's legitimate e-mail or the spoofed e-mail address to initiate unauthorized wire transfers.

In some cases, the funds from unauthorized wire transfers are directed to money mules[2] located in the United States. In other instances, wire transfers are directed to accounts of financial institutions outside of the United States. Victim reporting indicates criminal actors are starting to follow up on wire transfer requests by calling to confirm the transactions or to comply with wire transfer protocols, thus making the transaction appear more legitimate.

Other schemes seen in complaints filed with the Internet Crime Complaint Center (IC3) and in additional information made known to the IC3 indicates EAC money mules may be victims of employment scams, romance scams, or personal loan scams. It is not known why a specific victim is identified to be targeted.

Between 04/01/2015 and 06/30/2015, 21 complaints related to the EAC scam were filed with the IC3, with reported losses of almost $700,000. The FBI has identified approximately $14 million in attempted losses associated with open FBI EAC investigations.

EXAMPLES OF THE EAC SCAM ARE LISTED BELOW:

Financial/Brokerage Services –

- An individual's e-mail account is compromised by a criminal actor. The criminal actor, who is posing as the victim, sends an e-mail to the victim's financial institution or brokerage firm requesting a wire transfer to a person or account under the control of the criminal actor.
- An accounting firm's e-mail account is compromised and used to request a wire transfer from a client's bank, supposedly on behalf of the client.

Real Estate –

- A seller's or buyer's e-mail account is compromised through an EAC scam. The criminal actor intercepts transactions between the two parties and alters the instructions for the transfer of funds.

- A realtor's e-mail address is used to contact an escrow company to redirect commission proceeds to a bank account associated with the criminal actor.
- A realtor receives a link within an e-mail from an unknown person who is requesting information related to property. When the realtor clicks on the link, the criminal actor is able to access the realtor's e-mail account. The intrusion exposes client information, which the criminal actor then uses to e-mail the clients and attempt to change wire instructions for loan processing proceeds.

Legal -

- A criminal actor compromises an attorney's e-mail account, which results in the exposure of client bank account numbers, e-mail addresses, signatures, and confidential information related to pending legal transactions.
- The attorney's compromised e-mail account is used to send overlaid wire instructions to a client.
- A criminal actor compromises a client's e-mail account and uses it to request wire transfers from trust fund and escrow accounts managed by the firm.

WHAT TO DO IF YOU BELIEVE YOU HAVE BEEN A VICTIM OF THE EAC SCAM:

- Contact your financial institution immediately upon discovering the fraudulent transfer.
- Contact law enforcement.
- Request that your bank reach out to the financial institution where the fraudulent transfer was sent.
- File a complaint at www.IC3.gov, regardless of dollar loss. Provide any relevant information in your complaint and identify that your complaint pertains to the EAC scam.

TIPS TO PROTECT YOURSELF:

- Do not open e-mail messages or attachments from unknown individuals.
- Be cautious of clicking links within e-mails from unknown individuals.
- Be aware of small changes in e-mail addresses that mimic legitimate e-mail addresses.
- Question any changes to wire transfer instructions by contacting the associated parties through a known avenue.
- Have a dual step process in place for wire transfers. This can include verbal communication using a telephone number known by both parties.
- Know your customer. Be aware of your client's typical wire transfer activity and question any variations.

1.To learn more about how the BEC scam affects businesses, see the Public Service Announcement (PSA) dated 01/22/2015 at www.IC3.gov. It is anticipated that an updated BEC PSA will be released in August, 2015.↩

2.Money Mules are people who are used to transfer and launder stolen money. They are typically given a portion of the money transferred as payment. ↩

TLP:WHITE

NCCIC

Security Tip (ST04-014)

Avoiding Social Engineering and Phishing Attacks

Original release date: October 22, 2009 | Last revised: January 24, 2017

What is a social engineering attack?

> Do not give sensitive information to others unless you are sure that they are indeed who they claim to be and that they should have access to the information.

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

TLP:WHITE

TLP:WHITE

- Don't send sensitive information over the Internet before checking a website's security. (See Protecting Your Privacy for more information.)
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information.)
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft. (See Preventing and Responding to Identity Theft for more information.)
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission.

Author

US-CERT Publications

This product is provided subject to this Notification and this Privacy & Use policy.

TLP:WHITE



PHISHING TIP CARD

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information like account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access their accounts.

PHISHING EXAMPLES

The following messages, from the Federal Trade Commission's OnGuardOnline, are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit www.IRS.gov/uac/reporting-phishing.

SIMPLE TIPS

- **When in doubt, throw it out:** Links in email and online posts are often the way cybercriminals compromise your computer. If it looks suspicious – even if you know the source – it's best to delete or, if appropriate, mark it as "junk email." Contact the company directly (via phone) to be sure the email is not legitimate.
- **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- **Use stronger authentication:** Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username. Visit www.lockdownyourlogin.com for more information on stronger authentication.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.



- **Install and update anti-virus software.** Make sure all of your computers are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.
- **Be wary of hyperlinks:** Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over it to reveal the full address.

Stop.Think.Connect. is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™

TLP:WHITE

NCCIC

Security Tip (ST04-002)

Choosing and Protecting Passwords

Original release date: May 21, 2009 | Last revised: June 22, 2018

Why you need strong passwords

Passwords are a common form of authentication and are often the only barrier between you and your personal information. There are several programs attackers can use to help guess or "crack" passwords. But if you choose good passwords and keep them confidential, you can make it more difficult for an unauthorized person to access your information.

You probably use a number of personal identification numbers (PINs), passwords, and passphrases every day: from getting money from the ATM or using your debit card in a store, to logging in to your email or into an online retailer. Keeping track of all of the number, letter, and word combinations may be frustrating at times, but you've seen enough news coverage to know that hackers represent a real threat to your information. Often, an attack is not specifically about your account, but about using the access to your information to launch a larger attack.

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that those requesting access are the people they claim to be is the next step. This authentication process is more important and more difficult in the cyber world. Passwords are the most common means of authentication, but only work if they are complex and confidential. Many systems and services have been successfully breached because of insecure and inadequate passwords. Once a system is compromised, it's open to exploitation by other unwanted sources.

How to choose good passwords

Avoid common mistakes

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to crack them. Consider a four-digit PIN. Is yours a combination of the month, day, or year of your birthday? Does it contain your address or phone number? Think about how easy it is to find someone's birthday or similar information. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to dictionary attacks, which attempt to guess passwords based on common words or phrases.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "lITpbb" for "[l] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Changing the same example used above to "ll!2pBb." creates a password very different from any dictionary word.

Length and complexity

The National Institute of Standards and Technology (NIST) has developed specific guidelines for strong passwords. According to NIST guidance, you should consider using the longest password or passphrase

TLP:WHITE

TLP:WHITE

permissible (16–64 characters) when you can. For example, "Pattern2baseball#4mYmiemale!" would be a strong password because it has 28 characters. It also includes the upper and lowercase letters, numbers, and special characters. You may need to try different variations of a passphrase—some applications limit the length of passwords, some do not accept spaces or certain special characters. Avoid common phrases, famous quotations, and song lyrics.

Dos and don'ts

Once you've come up with a strong, memorable password it's tempting to reuse it – don't! Reusing a password, even a strong one, endangers your accounts just as much as using a weak password. If attackers guess your password, they would have access to all of your accounts. Use the following techniques to develop unique passwords for each of your accounts:

- Do use different passwords on different systems and accounts.
- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Use the longest password or passphrase permissible by each password system
- Don't use words that can be found in any dictionary of any language.
- Do develop mnemonics to remember complex passwords.
- Do consider using a password manager program to keep track of your passwords. (See more information below.)

How to protect your passwords

Now that you've chosen a password that's easy for your to remember, but difficult for others to guess, you have to make sure not to leave it someplace for people to find. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, is just making it easy for someone who has physical access to your office. Don't tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords. (See Avoiding Social Engineering and Phishing Attacks for more information.)

Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password. If you use a password manager, remember to use a strong master password.

Password problems can stem from your web browsers' ability to save passwords and your online sessions in memory. Depending on your web browsers' settings, anyone with access to your computer may be able to discover all of your passwords and gain access to your information. Always remember to log out when you are using a public computer (at the library, an Internet cafe, or even a shared computer at your office). Avoid using public computers and public Wi-Fi to access sensitive accounts such as banking and email.

There's no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.

For more information on passwords, multi-factor authentication, and related password topics, see Supplementing Passwords.

Don't forget security basics

- Keep your operating system, browser, and other software up-to-date.
- Use and maintain anti-virus software and a firewall. (See Understanding Anti-Virus Software and Understanding Firewalls.)
- Regularly scan your computer for spyware. (Some anti-virus programs incorporate spyware detection.)
- Use caution with email attachments and untrusted links.
- Watch for suspicious activity on your accounts.

TLP:WHITE

TLP:WHITE

Author
US-CERT Publications

This product is provided subject to this Notification and this Privacy & Use policy.

TLP:WHITE

TitleNews Online Archive

Sample Wire Fraud Warnings You Can Use

July 25, 2017

Title professionals are encouraged to remind clients about the risk of wire fraud. To combat this problem, title and settlement companies have:

- put consumer warnings on websites and communications OO used secured email communications
- sent notices to consumers and real estate agents informing them that the title companies' wire instructions will never change during the transaction
- called homebuyers and real estate agents on a known number to verify wire instructions before transmitting
- verified account holder information with the receiving bank prior to submitting a wire transfer

Here are examples of warnings to put in email signature lines:

- Be aware! Online banking fraud is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS call us immediately to verify the information prior to sending funds.
- Due to increased fraud, buyers, sellers and lenders should confirm all wiring instructions by phone directly with our office before transferring funds.
- WARNING! WIRE FRAUD ADVISORY: Wire fraud and email hacking/phishing attacks are on the increase! If you have an escrow or closing transaction with us and you receive an email containing Wire Transfer Instructions, DO NOT RESPOND TO THE EMAIL! Instead, call your escrow officer/closer immediately, using previously known contact information and NOT information provided in the email, to verify the information prior to sending funds.

Contact ALTA at 202-296-3671 or ***communications@alta.org****.*

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Understanding and Protecting Yourself Against Money Mule Schemes

Matthew DeSantis, Chad Dougherty, Mindi McDowell

Money Mules Are Used to Commit Fraud

"Money mules" are people who are used to transport and launder stolen money or some kind of merchandise. Criminals may even recruit money mules to use stolen credit card information. Individuals being used as money mules may be willing participants; however, many money mules are not aware that they are being used to commit fraud. The individuals being used as money mules are not the only victims; the larger scheme is designed to extract money from an organization or from other people.

Schemes May Seem Like Legitimate Opportunities

The most common money mule solicitations are disguised as "work from home" opportunities. These advertisements often target unsuspecting people who are interested in the convenience and flexibility of these types of jobs. Because there are companies that legitimately offer opportunities to work from home, users may not recognize malicious offers. Criminals often try to make the offer seem as legitimate as possible and may use the following approaches:

- carefully crafting the wording so that an email does not appear to be spam and is not caught by spam filters
- linking to fake but professionally designed websites that appear to belong to recognized companies or that promote a company that does not even exist
- posting some of these jobs on legitimate websites, including websites specifically for job seekers

Typical Process

After an individual agrees to be a money mule, the schemes tend to follow a similar process[1]:

1. The "company" collects information from the "employee." The information may include personal data such as the individual's Social Security number and bank account

[1] Bank Safe Online offers an illustration of this process (http://www.banksafeonline.org.uk/moneymule_explained.html).

© 2011 Carnegie Mellon University. Produced for US-CERT, a government organization.

information. The company may also ask the employee to sign a seemingly official contract.

2. The company (or the employee, under the direction of the company) creates a financial account[2] that the employee can use to collect and transfer funds.
3. The employee receives funds or some type of merchandise.
4. The employee is instructed to transfer the funds (usually keeping some percentage) to some other financial account or to deliver the merchandise to some third party. This financial account or third party is associated with the criminal. Often, the company will instruct the employee to use wire transfers for the funds, and there may be another money mule on the other end of the transfer with instructions to cash those funds.

Through this process, the criminal receives the stolen money or merchandise while hiding his or her involvement.

Typically, a criminal will only use a money mule once. After the money mule performs his or her role in the transaction, the criminal usually dissolves the relationship completely and recruits someone else for the next scheme.

Consequences Can Be Severe

If caught and prosecuted, the criminal faces the most severe consequences. However, the other parties involved in the scheme may also face serious consequences.

Money Mule

The following are potential consequences for money mules:

- **Inaccessible bank accounts** – During an investigation, law enforcement officials may freeze a money mule's bank accounts. Being unable to access funds may create a significant financial burden. These activities may also have a long-term impact on credit scores.
- **Prosecution** – Money mules may be prosecuted for their participation in these schemes.
- **Accountability for charges** – In some cases, money mules are found personally responsible for repaying the losses suffered by the other victims.[3]
- **Vulnerability of personal information** – As described in the typical process, criminals often collect personal information from the money mules. It is possible that the criminals may use this information for other malicious purposes.

[2] These accounts are typically established at a bank or through a service such as PayPal.

[3] "'Money Mules' Help Haul Cyber Criminals' Loot" (http://www.washingtonpost.com/wp-dyn/content/story/2008/01/25/ST2008012501460.html)

Targeted Individuals

If the fraud is designed to extract money from individuals, those individuals could experience the following consequences:

- **Financial loss** – An individual may pay for undelivered goods or have money deducted directly from one of his or her financial or credit card accounts. Depending on the forum used for the transaction and whether the scheme is identified, the individual may be able to recover at least a portion of these losses.
- **Significant hassle to resolve issues** – Identifying and reporting the fraud may require numerous steps, and the process could take a long time.

Targeted Organizations

If the fraud is designed to extract money from an organization, it may affect both the organization and its customers or constituents.

- **Financial loss** – A criminal may be able to siphon significant amounts of money from an organization's financial accounts before the activity raises suspicions.
- **Compromise of sensitive data** – If a criminal can access customer data, such as credit card information, he or she may be able to steal that information and use money mules to abuse the customers' financial or credit card accounts.
- **Damage to reputation** – If an organization experiences fraud, they may lose the trust and loyalty of their customers or partners.
- **Significant hassle to resolve issues** – Identifying and reporting the fraud may require numerous steps, and the process could take a long time.
- **Potential for future compromises** – If a criminal uses malicious code to access information on an organization's computer, he or she may hide additional malicious code that would allow the criminal to regain access in the future. If an organization does not locate and remove this code, it may be susceptible to another compromise.

Take Steps to Protect Yourself

Avoid Becoming a Money Mule

If an opportunity sounds too good to be true, it probably is. Look for common warning signs, and do some research before agreeing to participate. If you believe that you are participating in a money mule scheme, stop transferring money and merchandise immediately and notify the appropriate authorities. These authorities may include your bank, the service you used to conduct the transaction, and law enforcement.

Warning Signs

The following characteristics do not necessarily indicate a money mule solicitation, but they are commonly used in those solicitations[4].

- 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.

Research Strategies

- Perform online searches using information from the offer:
    - the subject line of the email
    - the company supposedly offering the position
    - the person who signed the message or the name of the contact person mentioned in the offer

  Look for indications that the offer might be a scam. If an online search does not produce any results, that may also be suspicious.
- Check the Better Business Bureau website[5].

Avoid Becoming a Victim

Individuals and organizations can both take precautions that minimize their risks.

Individuals

- Try to investigate the person or company before doing business with them.
- When transferring money, use a method that protects the transaction. For example, many banks, credit cards, and services such as PayPal may offer fraud protection.
- Monitor the transactions, including checking for withdrawals from your bank account and tracking an order.
- If you notice any problems, immediately contact the appropriate authorities. Depending on the circumstances, these authorities may include your bank, the service you used to conduct the transaction, and law enforcement.

---

[4] See the F-Secure Weblog for an example (http://www.f-secure.com/weblog/archives/archive-012007.html#00001084).

[5] http://www.bbb.org/

Organizations

Criminals typically use stealthy methods to access an organization's data or finances. These methods may include using malicious code, such as a virus, to gain administrative access to a computer within an organization or relying upon a malicious insider to transmit data or create fake customer accounts. By implementing the following precautions and practices, organizations may reduce their risk:

- Use anti-virus and anti-spyware software, and keep the definitions up to date.[6]
- Limit access to sensitive data to authorized personnel.
- Regularly check records, including employee lists and recent financial transactions. Look for new employees that Human Resources staff does not recognize, or for unauthorized transactions.
- Consider isolating the computers that perform banking and accounting functions. In small organizations, it may be feasible to use a separate laptop for these tasks. Larger organizations may be able to designate computers used to perform these tasks and apply stricter policies and access controls on those computers.
- Watch for suspicious behavior or activities from employees.[7]
- If you notice any problems, immediately contact the appropriate authorities. Depending on the circumstances, these authorities may include your IT department, your accounting department, and law enforcement.

Additional Resources

US-CERT Resources

- "Avoiding Social Engineering and Phishing Attacks" (http://www.us-cert.gov/cas/tips/ST04-014.html)

Other Resources

- Internet Crime Schemes: Employment/Business Opportunities (http://www.ic3.gov/crimeschemes.aspx#item-7)
- Money mule blog articles by Brian Krebs (http://krebsonsecurity.com/tag/money-mules)
- "Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams" (http://www.fsisac.com/files/public/db/p264.pdf)
- "Fraud Advisory for Businesses: Corporate Account Take Over" (http://www.fsisac.com/files/public/db/p265.pdf)

---

[6] See "Understanding Anti-Virus Software" (http://www.us-cert.gov/cas/tips/ST04-005.html) and "Recognizing and Avoiding Spyware" (http://www.us-cert.gov/cas/tips/ST04-016.html).

[7] The CERT® Insider Threat Center (http://www.cert.org/insider_threat/) offers insider threat resources for organizations.

Financial Fraud Kill Chain

Federal Bureau of Investigation
11 January 2016

Criminal actors are laundering billions of dollars overseas through financial fraud schemes like corporate account takeovers, business e-mail compromise scams, and other financially motivated crimes. The Financial Fraud Kill Chain (FFKC) is a process for recovering large international wire transfers stolen from US victim bank accounts. The FFKC utilizes FINCEN's relationship with the Egmont group, as well as federal law enforcement placement in countries all over the world to help stop the successful withdraw of cyber crime funds by criminal actors.

The FFKC is intended to be utilized as another potential avenue for US financial institutions to get victim funds returned. Normal bank procedures to recover fraudulent funds should also be conducted.

The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:

- the wire transfer is $50,000 or above;
- the wire transfer is international;
- a SWIFT recall notice has been initiated; and
- the wire transfer has occurred within the last 72 hours.

Any wire transfers that occur outside of these thresholds should still be reported to law enforcement but the FFKC cannot be utilized to return the fraudulent funds.

In order to initiate the FFKC, banks must provide the following information to their local FBI office.

Summary of the Incident:
Victim Name:
Victim Location (City, State):
Originating Bank Name:
Originating Bank Account Number:
Beneficiary Name:
Beneficiary Bank:
Beneficiary Account Number:
Beneficiary Bank Location (if available):
Intermediary Bank Name (if available):
SWIFT Number:
Date:
Amount of Transaction:
Additional Information (if available) - including "FFC"- For Further Credit; "FAV" – In Favor Of:

If the fraudulent funds are returned to the victim's account, the FBI requests that this information be passed back to their local field office contact.

Buyer's Fraud CHECKLIST

Begin the Transaction Securely

- Establish at least one trusted phone number for your real estate agent and settlement agent soon after your sales contract is signed.
- **Real estate agents** – phone numbers are often on the contract or listing agreement. You can also trust the brokerage's website or telephone directory.
- **Settlement agent** – you may get a letter or some other "opening" correspondence from the settlement agent. If you visit in person, pick up a business card. You can also trust the settlement agent's website or telephone directory. If your settlement agent is an attorney, their information can be obtained at www.flabar.org.
- Use a more "secure" email address for any correspondence about the transaction. Consider using your work email address because there are generally more firewalls and security protocols. Avoid free, internet-based accounts like Yahoo and Gmail.
- Do not send any personal or private information via email, including your social security number and identification documents. If you wouldn't share the information on Facebook, don't put it in your email!
- Verify any changes to the settlement agent's contact information or wiring instructions either in person or via the trusted phone number given at the beginning of the transaction.

End the Transaction Securely

- If you receive an email changing the timing and/or amounts to be wired to the settlement agent, verify using a trusted phone number or in person.
- Watch out for instructions marked "urgent" or giving a tight deadline (e.g. close of business today). Fraudsters want to create a sense of urgency to get you to act without thinking.
- Watch out for offers from the seller or their real estate agent that are "too good to be true." For example, if you are negotiating a repair escrow or credit at closing and receive an offer agreeing to resolution for significantly less money if they are paid the balance "today, by wire transfer," contact your real estate agent or attorney to verify the legitimacy of the offer.
- Never use the phone number given in an email to verify the information contained in the email. Fraudsters often use pre-paid cell phone numbers in these emails and then actually answer the phone when you call, thereby continuing the fraud.
- Be alert for slightly different email addresses from anyone connected with the transaction, for example:

  john-doe@bigbank.com vs.
  john-doebigbank@gmail.com
- If you are unable to verify the settlement agent's wire instructions via a trusted phone number or in person, wait until you can verify to wire funds.

© 2017 Attorneys' Title Fund Services, LLC.

Closer's Fraud CHECKLIST

Begin the Transaction Securely

- During your first interaction with each party to the transaction, establish at least one trusted phone number to use for contacting the person throughout the transaction.

  Consider at least one of the following methods:

  - Asking for the information in an engagement letter or intake form.
  - Using the contact information listed in the sales contract.
  - Asking for the information at an in-person meeting or during an incoming phone call.
  - DO NOT rely on telephone numbers solely provided via email. If in doubt, ask the party's real estate agent what phone number they use to contact the party directly.

- Alert buyer, seller and real estate agents in writing that they could be targets for email fraud.
  - Include in engagement or opening letter
  - Include in any emails (e.g., underneath the signature block) and other correspondence
- Inform parties they must verify any changes to contact information or disbursement or wiring instructions either in person or via the trusted phone number given at the beginning of the transaction.
- Inform all parties to not send private information via email, including social security numbers, identification numbers, and bank account information.
- Do not email wiring instructions. Send them via U.S. Mail or give them over the phone.
- If wiring instructions or other disbursement instruction changes are emailed to you, use the trusted phone numbers to verify.
- Inform the parties to the transaction that no monies will be disbursed until wiring instructions are confirmed over the phone.

End the Transaction Securely

- Review payoff and other wiring instructions slowly and carefully for inconsistencies.
- Obtain this information well in advance of closing to give yourself time to review and verify.
- Verify wiring instructions using the trusted phone numbers or in person.
- This includes payoffs to lenders or other creditors, real estate and mortgage brokers, as well as the sellers.
- Verify using a trusted phone number or in person if an email changes the timing and/or amounts to be wired.
- Watch out for instructions marked "urgent" or giving a tight deadline (e.g. close of business today). Fraudsters want you to abandon your verification routine by putting time pressures on you.
- Be alert for slightly different email addresses:

  john-doe@bigbank.com vs.
  john-doebigbank@gmail.com

- If you are unable to verify disbursement instructions via a trusted phone number, wait until you can verify to wire money or write a check.

© 2017 Attorneys' Title Fund Services, LLC.

Seller's Fraud CHECKLIST

Begin the Transaction Securely

- Establish at least one trusted phone number for your real estate agent and settlement agent soon after your sales contract is signed.
- **Real estate agents** – phone numbers are often on the contract or listing agreement. You can also trust the brokerage's website or telephone directory.
- **Settlement agent** – you may get a letter or some other "opening" correspondence from the settlement agent. If you visit in person, pick up a business card. You can also trust the settlement agent's website or telephone directory. If your settlement agent is an attorney, their information can be obtained at www.flabar.org.
- Use a more "secure" email address for any correspondence about the transaction. Consider using your work email address because there are generally more firewalls and security protocols. Avoid free, internet-based accounts like Yahoo and Gmail.
- Do not send any personal or private information via email, including your social security number and identification documents. If you wouldn't share the information on Facebook, don't put it in your email!
- Do not email your bank account wiring instructions. Instead, send them via U.S. Mail, give them over the phone, or take them in person to your real estate or settlement agent.
- If your wiring instructions change after you originally provide them, deliver the new instructions to your real estate or settlement agent in person.
- Learn about and understand the settlement agent's policy on disbursement. Many settlement agents require oral verification of wire instructions before disbursement.

End the Transaction Securely

- Contact your bank to obtain your account's wire instructions well in advance of closing.
- Watch out for offers from the buyer or their real estate agent that are "too good to be true." For example, if you are negotiating a repair escrow or credit at closing and receive an offer agreeing to resolution for significantly less money if they are paid the balance "today, by wire transfer," contact your real estate agent or attorney to verify the legitimacy of the offer.
- Never use the phone number given in an email to verify the information contained in the email. Fraudsters often use pre-paid cell phone numbers in these emails and then actually answer the phone when you call, thereby continuing the fraud.
- Be alert for slightly different email addresses from anyone connected with the transaction, for example:

  john-doe@bigbank.com vs.
  john-doebigbank@gmail.com
- Make sure you are available by phone or in person at closing to verify wire instructions.

© 2017 Attorneys' Title Fund Services, LLC.

Information Security FAQs

E-Mail Security

E1. I just received an e-mail from the seller in a current transaction directing me to wire the sales proceeds to their account. This is the first communication I have received with wire instructions. Should I follow the directions?

E2. I received an e-mail directing me to wire proceeds from a sale to a "new" account. I noticed that the return e-mail address is not exactly correct. I called the seller and he did not send the e-mail. What do I do now?

E3. My e-mail was hacked – what do I do?

E4. What is two-factor authentication?

E5. The buyer called to verify that we received the deposit via wire per our e-mail instructions. The problem is that we did not send any such request. What should we do?

E6. I opened an e-mail which simply stated "here is the closing file you requested." Nothing was attached and there was no reference to a particular file. I tried to respond to the e-mail, but have not yet received a response. Is there something I should do in the mean time?

E7. Are fake e-mails easy to spot?

E8. What steps should we take to protect ourselves and our clients from a potential e-mail scam?

E9. Is e-mail encryption required?

Trust Account Security

T1. I received a cashier's check as part of a deposit for an upcoming transaction. The buyer is now asking for part of the funds to be returned by wire transfer because the check was for more than the required deposit. May I go ahead and refund the difference?

T2. I received a call from the seller's lender telling me to wire the payoff funds in a specific transaction to a different bank account. The caller knew all of the details about the transaction, including the closing date, payoff amount, per diem, and seller's account number. Can this still be fraud?

T3. What is the difference between wired funds and automated clearinghouse transfers (ACH)?

T4. Do I have to complete background checks on my employees who have worked for me for a long time?

Fraudulent Transactions

F1. I am opening a new file and something does not seem right. The buyer stated he learned about our firm on the internet, he is not currently residing in the United States, and he is sending the deposit check directly to our firm. What should I check?

F2. Are there any places that I can sign up for notices of the latest information security threats and issues?

F3. What resources are available for more information?

E-Mail Security

E1. I just received an e-mail from the seller in a current transaction directing me to wire the sales proceeds to their account. This is the first communication I have received with wire instructions. Should I follow the directions?

A. Not without additional verification. It is common for hackers to gain access to sellers', buyers', and real estate agents' e-mail accounts. Before wiring any funds pursuant to e-mailed instructions, call the seller on a number which you have been previously provided to verify the information. Be careful not to use telephone numbers provided in the e-mails, as fraudsters will provide fake phone numbers in the hope you will call the fake phone number and continue with the transaction.

You should also consider requiring the seller to come to your office and sign a change authorization or wire instruction form. At that time, you can obtain a copy of their identification as verification that they truly are the seller.

This is a new area of concern for many real estate agents and sellers so you should consider setting out your office policy on obtaining and changing wire instructions at the beginning of the transaction so as not to cause any party unnecessary delay on or after the closing date.

E2. I received an e-mail directing me to wire proceeds from a sale to a "new" account. I noticed that the return e-mail address is not exactly correct. I called the seller and he did not send the e-mail. What do I do now?

A. Report the incident to:

- The Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3). IC3's mission is to provide a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected internet-facilitated criminal activity. IC3 will request the following information (if known):
    - Victim's name, address, telephone, and e-mail.
    - Financial transaction information (e.g., account information, transaction date and amount, and who received the money).
    - Subject's name, address, telephone, e-mail, website, and IP address.
    - Specific details on how you were victimized.
    - E-mail header(s).
    - Any other relevant information you believe is necessary to support your complaint.

- Federal Trade Commission (FTC)
- US Secret Service (USSS)
- Real estate brokers should report to their state or local REALTOR® association.

E3. My e-mail was hacked – what do I do?

A. You should follow the steps below if you have been a victim of e-mail hacking:

1. Update or install security software from a company you trust with automatic updates.
2. Change your password and set up two-factor authentication (Outlook and Microsoft, Google, Yahoo).
3. Change your security questions and make the answers as creative as possible (try to avoid questions and answers that are easily obtained through social media platforms such as mother's maiden name, names of pets, high school attended, hometown, etc.).
4. Report the incident to your e-mail provider, IC3, FTC, and USSS.
5. Notify everyone on your contact list.
6. Scan your computer with an updated anti-virus program – delete anything suspicious and re-start your computer.
7. Check your e-mail settings to make sure no one added any links to your signature and that your e-mails are not being forwarded to someone else.
8. Change passwords or security questions for other sites (especially those where you use the same password and security questions!).
9. Check your e-mail folders – search for "password" to see what other compromises might have happened.
10. Monitor your credit and financial accounts for fraudulent activity.

E4. What is two-factor authentication?

A. Two-factor authentication is a method of confirming a user's claimed identity by utilizing a combination of two different components. In most e-mail two-factor authentication schemes both a "knowledge factor" and a "possession factor" are used. The "knowledge factor" is something that the user knows, typically the password to the e-mail account. The "possession factor" utilizes something the user possesses, typically a cell phone. In a common two-factor authentication scheme, a user will enter the password to the e-mail account. The correct password will trigger a text message to the phone number previously provided by the user with a one-time verification code contained therein. The user must then provide the verification code to the e-mail server within a specified time period to be granted access to the account.

E5. The buyer called to verify that we received the deposit via wire per our e-mail instructions. The problem is that we did not send any such request. What should we do?

A. Instruct the buyer to contact his bank immediately to try to retrieve the wire. Depending on the circumstances wires can be retrieved up to 72 hours after they are sent. The buyer should also report the crime to IC3, FTC, and USSS. Some banks may require this reporting to law enforcement during the recovery process.

To cut down on the possibility of future occurrences, you might consider including information in your introductory letter to the parties about how they will receive information about deposits and wire instructions from you. This introductory letter should be sent via U.S. Mail to cut down on the possibility that it will be intercepted by a fraudster from a compromised e-mail account.

E6. I opened an e-mail which simply stated "here is the closing file you requested." Nothing was attached and there was no reference to a particular file. I tried to respond to the e-mail, but have not yet received a response. Is there something I should do in the mean time?

A. Unsolicited e-mail may contain malware which will download to your computer if the e-mail is opened. Some malware is designed to record keystrokes in order to determine passwords to sensitive websites, such as online banking or other financial institutions. If you open an e-mail like this one, contact your IT department for assistance.

Some steps you or your IT department can take are:

- Take the computer off the network until it can be secured.
- Scan your computer looking at all programs that have been installed. Delete any program that you did not install.
- Check the server and all other computers on the network to make sure no other machines have been affected.
- Change all passwords. This includes passwords to online accounts accessed at that computer.
- Make any needed updates to your anti-virus software and firewalls.

E7. Are fake e-mails easy to spot?

A. Unfortunately, no, fake e-mails can be very elaborate. Some Fund Members have received e-mail ostensibly from an attorney requesting that a deposit be wired into a phony trust account. These e-mails may contain the buyers', sellers', and real estate agents' information as well as the property address, sales price, and attorney's e-mail address. Some of these e-mails also contain phone numbers that, if called, will put the caller directly in touch with the fraudster who will verify the requested information. Receiving fake e-mail does not necessarily mean that someone's e-mail account has been hacked. Fraudsters can gather this information from social media accounts or by accessing the Multiple Listing Service.

E8. What steps should we take to protect ourselves and our clients from a potential e-mail scam?

A. A couple of very basic steps will help:

- Notify all parties to the transaction of your policies regarding e-mail usage, changes to wire instructions, and changes to contact information including telephone numbers.
- Exchange telephone numbers early in the transaction and insist upon oral verification of important communications. If a party's telephone number changes over the course of the transaction, have procedures in place to verify the accuracy of the new phone number and the authority of the person making the change. The party may need to appear in person to provide the new number.
- Do not use telephone numbers provided in e-mails unless their authenticity has been confirmed.
- Verbally verify with the recipient all outgoing wiring instructions prior to initiating the wire.
- Take caution when opening e-mail attachments from supposed parties to the transaction. If in doubt as to identity of sender, call and confirm it was sent by them.

Tips on spotting phony e-mail:
Carefully review the sender's e-mail address against the e-mail address you have on file. For example, if a party's e-mail address is joesmith@abccompany.com, look for slight variations such as extra or missing characters, or different domains. Note how the following e-mail addresses are subtly different: joe.smith@abccompany.com, joesmith@abcompany.com, joe_smith@abccompany.com, or joesmith@abccompany.net.

You may need to hover your cursor over the sender's e-mail address in order to see the entire address and not the nickname associated with the account, e.g. "Joe Smith."

E9. Is e-mail encryption required?

A. The TILA-RESPA Integrated Disclosure (TRID) rule does not require e-mail encryption. However, other federal privacy laws enforced by the CFPB require the protection of non-public personal information (NPI). If sending NPI via e-mail, encryption or other security procedures are advisable.

In addition, lenders may require e-mail encryption in correspondence with the lender or its borrower. Inquire with the lenders you work with often to see if they require your e-mail to be encrypted. If you are not required by the lenders you work with, it then simply becomes a business decision for you on whether or not you want to encrypt none, some, or all of your e-mail.

Trust Account Security

T1. I received a cashier's check as part of a deposit for an upcoming transaction. The buyer is now asking for part of the funds to be returned by wire transfer because the check was for more than the required deposit. May I go ahead and refund the difference?

A. No. Do not refund any part of the deposit until you have collected funds. There are many fraudulent cashier's check schemes as well as fake law firm trust account checks, fake corporate checks, and more. This is one of the more common schemes that have been reported.

T2. I received a call from the seller's lender telling me to wire the payoff funds in a specific transaction to a different bank account. The caller knew all of the details about the transaction, including the closing date, payoff amount, per diem, and seller's account number. Can this still be fraud?

A. Yes, it can still be fraud. It is not likely that a seller's lender will unilaterally change the payoff instructions prior to closing. In the rare case where this might occur, the lender will typically send any changes to the payoff instructions in writing. When dealing with payoff information, establish contact information early in the transaction and rely on that information to verify changes. If you happen to receive a change to the payoff instructions from a lender or other creditor, always call the institution to verify the changes. Make sure to contact the institution using a phone number from its publicly available website, not the phone number listed on the suspicious payoff instructions, fax cover page, or e-mail correspondence.

T3. What is the difference between wired funds and automated clearinghouse transfers (ACH)?

A. Wired funds are monies that pass directly from one financial institution to another financial institution using the Federal Reserve's Fedwire system.

ACH transfers are similar to an electronic check and use a "batch" system of payment. The batch system means that instead of each transaction being handled individually as in a wire transfer, all the ACH transfers are sent to a centralized clearinghouse, held for a period of time, and then sent to the receiving bank at once in a batch. This means that multiple transactions are processed simultaneously once or multiple times a day, depending on the bank.

Wire transfers are generally more expensive than ACH transactions, many of which have no additional cost associated with them. However, ACH transactions can take longer to process, because of their batch characteristics and they are less secure than wire transfers. The identities of both the initiating and receiving parties to a wire transfer are generally verified, making a wire much harder to "fake."

T4. Do I have to complete background checks on my employees who have worked for me for a long time?

A. The American Land Title Association's Best Practices recommend five-year background checks be performed every three years on employees who have access to the trust accounts. It also recommends that a five-year background check be completed on all new hires who will have access to the trust accounts.

Fraudulent Transactions

F1. I am opening a new file and something does not seem right. The buyer stated he learned about our firm on the internet, he is not currently residing in the United States, and he is sending the deposit check directly to our firm. What should I check?

A. This gut feeling could happen for any number of reasons. Below are some items to consider:

- If a real estate agent is participating in the transaction, give them a call. (Do not e-mail the real estate agent as the agent's e-mail may have been compromised, which is potentially how you were brought into the transaction.) Ask the real estate agent if they met the buyer in person or were also contacted online.
- Require more than one form of identification before accepting the employment. Make copies and re-check the identification at closing.
- Contact the record owner of the property and verify the sale. (Obtain seller contact information independently of the real estate agent and buyer.)

F2. Are there any places that I can sign up for notices of the latest information security threats and issues?

A. Yes, there are several. These organizations provide period e-mail updates on information security threats:

- Federal Bureau of Investigation
- Internal Revenue Service
- Federal Trade Commission – to receive scam alerts
- National Cyber Awareness System Mailing Lists – from the United States – Computer Emergency Readiness Team

F3. What resources are available for more information?

- Federal Financial Institutions Examination Council -Cybersecurity Awareness page with many links as well as Cybersecurity Assessment Tool
- Federal Bureau of Investigation – information on scams and safety on the internet and how to protect your computer
- Federal Trade Commission – Start with Security: A Guide for Business

The Florida Bar

651 East Jefferson Street
Tallahassee, FL 32399-2300

Joshua E. Doyle
Executive Director

850/561-5600
www.FLORIDABAR.org

Certificate of Accreditation for Continuing Legal Education

256131
Attorney's Title Fund Services
Robert Rohan
PO Box 628600
Orlando, FL 32862-8600

November 14, 2018

Reference Number:	1808489N
Title:	Stopping Cyber Fraud
Level:	Intermediate
Approval Period:	12/14/2018 - 06/14/2020

CLE Credits

General	1.0
Ethics	1.0
Technology	1.0

Certification Credits

Business Litigation	1.0
Real Estate	1.0

NALA | THE PARALEGAL ASSOCIATION

7666 E. 61st, Suite 315, Tulsa, OK 74133
Phone: 918-587-6828 ♦ Fax: 918-582-6772
www.nala.org ♦ cle@nala.org

CERTIFICATE OF ATTENDANCE

Certified Paralegals are required to submit evidence of 50 hours of continuing legal education hours to renew the CP credential every 5 years. Of the 50 hours, 5 hours must be in legal ethics, and no more than 10 hours may be recorded in non-substantive areas. If attending a non-NALA sponsored educational event, this certificate should be completed and submitted with relevant documentation for the event. Please be sure to obtain the required signatures for verification of attendance. The requirements to maintain the CP credential are available from NALA's web site at https://www.nala.org/certification/certtest2view.

PLEASE COMPLETE THE SPACES BELOW AND ATTACH A PROGRAM

Session Hours	Session Topics (Description and Speakers)	Validation of Attendance
1.0	Wire transfer fraud/Rohan	*RR*

Name of CP (Please Print)

NALA Account Number (On Mailing Label)

Signature of CP

Stopping Cyber Fraud
Name of Seminar/Program Sponsor

Address

Robert Rohan
Authorized Signature of Sponsor Representative

Date of Educational Event:

Preferred e-mail address

Online webinar
Location:

For Office Use Only	
Substantive hours	
Non-substantive hours	
Ethics	