Information Security FAQs

Email Security 2

E1. I just received an email 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? 2

E2. I received an email directing me to wire proceeds from a sale to a "new" account. I noticed that the return email address is not exactly correct. I called the seller and he did not send the email. What do I do now? 2

E3. My email was hacked – what do I do? 3

E4. What is two-factor authentication? 3

E5. The buyer called to verify that we received the deposit via wire per our email instructions. The problem is that we did not send any such request. What should we do? 3

E6. I opened an email 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 email, but have not yet received a response. Is there something I should do in the meantime? 4

E7. I am concerned that my office may have been the victim of a phishing attack. What can I do to protect myself? 4

E8. Are fake emails easy to spot? 4

E9. What steps should we take to protect ourselves and our clients from a potential email scam? 5

E10. Is email encryption required? 5

Trust Account Security 6

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? 6

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? 6

T3. What is the difference between wired funds and automated clearinghouse transfers (ACH)? 6

T4. Do I have to complete background checks on my employees who have worked for me for a long time? 6

Fraudulent Transactions 7

F1. I am opening a new file and something does not seem right. The buyer stated he learned about our business on the internet, he is not currently residing in the United States, and he is sending the deposit check directly to our business. What should I check? 7

F2. Are there any places that I can sign up for notices of the latest information security threats and issues? 7

F3. What resources are available for more information? 7

Email Security

E1. I just received an email 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' email accounts. Before wiring any funds pursuant to emailed 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 emails, 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 email directing me to wire proceeds from a sale to a "new" account. I noticed that the return email address is not exactly correct. I called the seller and he did not send the email. 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 email.
    - Financial transaction information (e.g., account information, transaction date and amount, and who received the money). o Subject's name, address, telephone, email, website, and IP address.
    - Specific details on how you were victimized. o Email 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 email was hacked – what do I do?

A. You should follow the steps below if you have been a victim of email 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 email 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 restart your computer.
7. Check your email settings to make sure no one added any links to your signature and that your emails 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 email 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 email 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 email 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 email 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 email 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 email instructions. The problem is that we did not send any such request. What should we do?

A. Instruct the buyer to contact their 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 email account.

E6. I opened an email 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 email, but have not yet received a response. Is there something I should do in the meantime?

A. Unsolicited email may contain malware which will download to your computer if the email 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 email 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 on that computer.
- Make any needed updates to your anti-virus software and firewalls.

E7. I am concerned that my office may have been the victim of a phishing attack. What can I do to protect myself?

A. Whether your office has been a phishing victim or not, you (or your IT department) should analyze your email settings regularly to determine if fraudsters have created auto-forwarding rules that allow them to hijack emails and monitor your communications. Their intent is to insert real-looking but fraudulent emails to redirect pending or future payments. The FBI released a Private Industry Notification (PIN) addressing this very threat with recommended mitigation techniques. The PIN can be found here.

E8. Are fake emails easy to spot?

A. Unfortunately, no, fake emails can be very elaborate. Some agents have received email ostensibly from an attorney requesting that a deposit be wired into a phony trust account. These emails may contain the buyers', sellers', and real estate agents' information as well as the property address, sales price, and attorney's email address. Some of these emails also contain phone numbers that, if called, will put the caller directly in touch with the fraudster who will verify the requested information.

Receiving a fake email does not necessarily mean that someone's email account has been hacked. Fraudsters can gather this information from social media accounts or by accessing the Multiple Listing Service.

E9. What steps should we take to protect ourselves and our clients from a potential email scam?

A. A couple of very basic steps will help:

- Notify all parties to the transaction of your policies regarding email 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 emails unless their authenticity has been confirmed.
- Verbally verify with the recipient all outgoing wiring instructions prior to initiating the wire.
- Take caution when opening email attachments from supposed parties to the transaction. If in doubt as to the identity of the sender, call and confirm it was sent by them.

Tips on spotting phony email:

- Carefully review the sender's email address against the email address you have on file. For example, if a party's email address is joesmith@abccompany.com, look for slight variations such as extra or missing characters, or different domains. Note how the following email 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 email address in order to see the entire address and not the nickname associated with the account, e.g. "Joe Smith."

E10. Is email encryption required?

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

In addition, lenders may require email encryption in correspondence with the lender or its borrower. Inquire with the lenders you work with often to see if they require your email 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 email.

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 email 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 business on the internet, he is not currently residing in the United States, and he is sending the deposit check directly to our business. 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 email the real estate agent as the agent's email 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 at least two forms of identification before accepting the engagement. Retain copies of the identification documents and verify the individual's identity again 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 periodical email 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