ALLIANT NATIONAL
TITLE INSURANCE COMPANY

ESCROW FRAUD/SOCIAL ENGINEERING

RECENT SCHEMES AND PREVENTION TIPS

INTRODUCTION

Escrow fraud accomplished via social engineering continues to be a major threat to title agents, real estate agents, lenders and consumers. Title agents across the country are reporting a surge in attempted wire fraud, and local news outlets increasingly are sharing the stories of devastated consumers who unwittingly have sent seller proceeds to fraudsters. Alliant National is closely monitoring the situation and is committed to providing updated, timely information to help our agents protect their businesses and the consumers they serve.

The threat from fraudsters is great, and no one policy or technology solution will ensure the safety of escrow funds. For this reason, we offer the following information, tips and suggestions to help our agents better understand the current threat environment and create a comprehensive plan that addresses the realities we face.

This document addresses five basics questions at the heart of the escrow fraud issue.

IDENTIFY	**PROTECT**	**DETECT**	**RESPOND**	**RECOVER**
What are the risks we face?	What steps can I take to protect my agency?	How can I spot attempted social engineering and wire fraud?	What do I do if I spot attempted social engineering and wire fraud?	How do I recover if my agency falls victim to wire fraud?

**Adapted from the National Institute of Standards and Technology (NIST) Cybersecurity Framework. www.nist.gov/cyberframework.*

To beat the bad guys, we need to work together as an industry and in partnership with all stakeholders in the real estate transaction including consumers, real estate agents and lenders. This document places special emphasis on subjects title agents may want to discuss with others.

Fraudsters are notorious for finding the weakest link in the security chain, and we commend our agents who have taken a leadership role in ensuring all parties to the transaction are aware of the current fraud threat and know how they can help keep escrow funds secure.

IDENTIFY

What are the risks we face from social engineering and wire fraud?

Alliant National agents continue to report an increase in attempted wire instruction fraud schemes. Some schemes have proven successful and resulted in substantial dollar losses. Thankfully, quick action by agents and banks has led to recovery of funds in some cases.

These attacks are part of a growing fraud threat targeting businesses of all sizes and the general public. The FBI refers to this threat as Business Email Compromise/Email Account Compromise (BEC/EAC). As the name implies, BEC scams are carried out by compromising legitimate business email accounts. The EAC component of the scam refers to the targeting of consumers and the lenders, real estate professionals, attorneys and others who serve them.

BEC/EAC fraudsters focus on organizations that perform wire transfers. According to the FBI's Internet Crime Complaint Center (IC3), BEC/EAC scams have been reported by businesses and victims in all 50 states and in 131 countries. IC3 data indicates fraudsters stole or attempted to steal more than $1.59 billion from roughly 22,000 U.S. victims between October 2013 and December 2016. Fraudulent transfers have been sent to 103 countries with the majority going to Asian banks located in China and Hong Kong.

IC3 saw a 480 percent increase in the number of complaints in 2016 filed by title companies that were the primary targets of BEC/EAC scams.

BEC/EAC Scams Have Been Reported in

ALL 50 STATES 131 COUNTRIES

The Majority of Fraudulent Transfers Go To

ASIAN BANKS IN CHINA AND HONG KONG

BEC/EAC scams in the title industry overwhelmingly involve attempts to divert wires. However, the FBI warns that BEC/EAC scammers increasingly are targeting organizations with the primary goal of obtaining personally identifiable information (PII) or wage and tax statement (W-2) forms for employees.

Given the current nationwide threat climate, we encourage all agents and their staff to remain on **high alert** for attempted fraud, particularly when it comes to seller proceeds. We also urge agencies to remain vigilant regarding possible attempts to obtain consumer or employee PII.

Maintaining policies and procedures for verification of wire instructions is critical in this environment. Many Alliant National agents have successfully confronted the threat by establishing plans to quickly

detect fraud and recover diverted funds. Obtaining appropriate insurance (as discussed later), including Cyber-Liability coverage also is essential given the threats we face.

To combat fraud, we believe it's important to work together. We have established the Alliant National Fraud Hotline email box fraudhotline@alliantnational.com to be a clearinghouse for information on burgeoning fraud trends and threats. You're encouraged to tell us about instances of fraud or attempted fraud you've heard about or observed. We are only interested in sharing information on the nature of these fraud threats, so names and other identifying information will be kept confidential. Fraud information provided to us will be disseminated to agents around the country for the purpose of raising awareness regarding the latest schemes. However, if the insured under the policy is a potential victim of fraud, please contact the Alliant National Claims Department immediately at 877-788-9800, ext. 425, or submit a claim to Alliant National at claims@alliantnational.com.

SCHEMES: VARIATIONS ON AN IMPERSONATION THEME

BEC/EAC wire fraud schemes usually involve an element of "social engineering," which typically mixes deception and impersonation to manipulate victims into revealing sensitive information, transferring funds or granting computer access to the fraudster (for more information on social engineering fraud, see Special Alert 15-08).

Exactly how certain victims are targeted is not known, but IC3 has warned companies to be careful about what they post on social media and on their websites. Information about job duties, leadership structure and out-of-office details can give scammers the basic information they need to start building a web of deceit.

IC3 has noted that BEC/EAC victims may first receive "phishing" emails seeking details on the targeted business or individual; these emails purport to be genuine in order to fool others into providing sensitive information. Victims may receive "spoofed" emails from seemingly legitimate sources that contain malicious links or code. Fraudsters posing as technology vendors or other legitimate contacts will also telephone businesses seeking information about technology platforms and key employees.

BEC/EAC wire fraud schemes involving settlement agents can vary in the details but tend to follow common patterns. ***Often, fraudsters hack the email account of the real estate agent or another party and monitor the account for upcoming real estate closings (Special Alert 14-01). As a closing date approaches, the fraudsters — posing as one of the parties to the transaction — interject themselves into the communications chain and seek to change wire instructions.***

Fraudulent communications usually come via email but also can be made via telephone or fax. Criminals have become extremely proficient at pretending to be other people — sometimes going so far as to mimic someone in the transaction while delivering bogus wire instructions to the settlement agent over the phone. **Here are a few of the schemes we have heard about from our agents.**

1. **THE SELLER SPOOF:** A classic. Fraudsters, posing as the seller, email the settlement agent using an email address that looks like the seller's, or even uses the seller's actual email address. The criminals attempt to divert seller proceeds to a fraudulent account (Special Alert 16-01).

2. **THE LATE SWITCHEROO:** The settlement agent receives instructions from the seller regarding where to wire the seller's sale proceeds. Then, before the closing, the settlement agent receives a message from an email address that looks like it is from the real estate agent instructing the settlement agent to wire the sale proceeds to a different, fraudulent account (Special Alert 15-01).

3. **EARNEST MONEY HUSTLE:** The settlement agent receives an email from an address that appears to be the real estate agent's. The fraudster instructs the settlement agent to release the earnest money deposit back to the alleged client. The instructions direct funds to a fraudulent account (Special Alert 14-01).

4. **THE BUYER BEWARE:** Fraudsters pose as the settlement agent or real estate agent using an email address that looks like it is from one of them and instruct the buyer to wire his or her down payment funds to a fraudulent bank account (Special Alerts 14-01, 15-03 and 16-02).

5. **THIRD-PARTY POOPER:** In a transaction involving a third-party investor who is to receive seller proceeds: The fraudsters, impersonating the investor, using an email address that looks like the investor's, provide fraudulent wire instructions to the seller. The seller conveys these instructions to the settlement agent who wires proceeds to the fraudulent account.

In addition, some frauds may not involve the buyer, seller or real estate agent. Here are some examples:

6. **BUSINESS EXECUTIVE SCAM:** Fraudsters, posing as the CEO or CFO of a title company, email an employee whose job includes transferring funds. The email requests an urgent payment to be made outside of normal procedures, often giving a pressing reason. The account to which payment is made is fraudulent (Special Alert 15-07).

7. **THE VENDOR BENDER:** Fraudsters, posing as a vendor of the title company, email the title company directing payment of an invoice to a fraudulent account (Special Alert 15-07).

PROTECT

What steps can I take to protect my agency?

As our agents have observed, fraudsters will attempt to impersonate any party to the transaction in a position to alter wire instructions. That's why all of us must continually educate buyers, sellers, real estate agents and others about how everyone in the transaction can work together to lessen the risks.

The FBI urges businesses to verify money transfer instructions using "Out of Band" communications. That simply means establishing other communication channels, such as telephone calls, to verify transactions. Many agents find it helpful to discuss and confirm these verification processes with consumers at or near the time an order is received — and not via email.

Verification procedures for wire transfer instructions are important, but as we all know, any procedures are only as good as the training we provide to our staff members. Even the best prepared agencies can fall victim to a scam. That's why making fraud prevention a part of both a written security program *and* the company culture is essential.

What specific steps can agents take to protect themselves? Here are some good business practices our agents have shared with us that you may want to consider. We have discussed many of these in previous alerts. Agents who have adopted these and other policies tell us it is helpful to discuss them with consumers when the file is first opened. That way, consumers can be prepared for these procedures and are themselves empowered to understand and respond to the security issues involved in real estate transactions.

- Some agents generally decline to accept instructions to wire seller proceeds without a form physically signed by the seller to which a voided check from the indicated account is attached. (Special Alert 16-01).
- We consider it a best practice to decline to accept any wire instructions, or changes to wire instructions, merely on the basis of an email, fax, inbound telephone call or other form of electronic communication. In the event instructions are received via email or fax, a best practice is to accept the instructions only after verifying the information using a verified telephone number. Agents often discuss this policy with consumers when the order is placed and obtain this verified number on a document at that time. Then, when an email or other electronic communication needs to be verified, they refer to this document and not to numbers that may appear on emails or in other communications.
- To verify wire instructions by phone, some agents have shared that they use a pre-determined PIN code or challenge question. As in the case of the verified telephone number, this process is

discussed with the consumer when the file is first opened, and the information is collected at that time. The PIN or challenge question is never communicated electronically. Emailing, texting or faxing this information, or leaving it on a voicemail, may limit its usefulness as an independent means of verification. A party calling to confirm or change security measures must come into the title company with appropriate identification.

- Some agents have told us they will not provide a copy of a wire confirmation (which contains all of the customer's bank account information) to anyone on the basis of an unconfirmed email, fax, text or inbound telephone call (Special Alert 16-01).
- Fraudsters will attempt to hack, spoof and impersonate any party involved in the communication of wire instructions. Some agents attempt to lessen this risk by communicating wire instructions directly with consumers without routing them through real estate agents. Doing so protects the real estate agent and the consumer. It is helpful to discuss such policies with consumers and real estate agents in advance (Special Alerts 14-01 and 15-01).
- Some agents will only provide wire instructions to consumers in person or via encrypted email using a password protected PDF where the password was selected by the recipient in person at the opening of the file. Again, care is taken not to email, fax or text the password, or provide it over the phone.
- The FBI recommends that businesses refrain from using the "Reply" option to respond to emails. This tip may be particularly useful when communicating about wire instructions. Instead, the FBI suggests using the "Forward" option and either typing in the correct email address or selecting it from the email address book to ensure the intended recipient's correct email address is used.
- Because fraudsters can strike anywhere in the communications chain, consumers play an important role in helping protect funds. Consider encouraging consumers to whom you send closing instructions to contact you by phone if they receive any further contact attaching wiring instructions, even if the instructions appear to be coming from the closing agent. Of course, the number the consumer calls should be a verified number and not a number displayed on a suspect email.
- Consumers also should be wary of any email purporting to be from a closing agent or another party to the transaction that has a generic domain at the end, like "gmail" or "mail" (Special Alert 15-03).
- We consider it a best practice to wire only to accounts that match information on the Closing Disclosure Form. If the information differs, special care is warranted to verify the consumer's identity and information (Special Alert 16-01).
- Some agents follow a two-step verification process prior to sending a wire: Telephone verification by the processor and final telephone verification by the wire department. The reasoning behind the policy is explained to consumers and real estate agents in advance.

- Some agents prefer to send wires in batches or have instituted a "mellow period" so wires are not sent immediately after verification of instructions. Fraudsters often attempt to use pressure tactics to influence agency employees, so if a consumer or other party is greatly upset by this procedure, some agents treat that response as a potential red flag.
- Take special care to verify the identity of parties when a transaction involves out of state or international consumers.
- Our agents observe that BEC schemes often originate with a hack of the real estate agent's email account. As such, we encourage you to dialog with your real estate agent clients about this threat (Special Alerts 14-01 and 15-01).

A consumer buying or selling a home often feels excited about completing the transaction and is eager to move on with the next phase of life. Fraud is likely the last thing on the consumer's mind. Title agents are in a unique position to help consumers understand the dangers of fraud and the steps they can take to protect their funds and personal information.

Do tell!

- **TELL THE CONSUMER** that fraudsters are targeting buyers and sellers and that unwitting consumers have been scammed into wiring funds to fraudsters. Tell them to be wary of any email purporting to be from a closing agent or another party to the transaction that has a generic domain at the end, like "gmail" or "mail."
- **DISCUSS YOUR COMPANY'S PROCEDURES** for accepting, verifying and changing wire instructions. Establish any pin codes or challenge questions you might use to identity the consumer should they call your agency.
- **TELL THE CONSUMER** that if they receive an email from your agency regarding wiring funds, they should verify the information by contacting your office using a pre-determined telephone number and not a number that might appear on the email.
- **DISCOURAGE THE CONSUMER** from sharing wiring instructions or other banking information with third parties, including the real estate agent.
- **MOST OF ALL, LET THE CONSUMER KNOW** they should never wire funds based on an email, even if the emails appears to come from the title company, the real estate agent, the bank or anyone else.

DETECT

How can I spot attempted social engineering and wire fraud?

Many agents report seeing a steady stream of potentially fraudulent emails and communications. Continual evaluation of internal and external communications is recommended. Below are some tips for sniffing out bogus emails and phone calls. It bears repeating that fraudsters will target anyone in the communications chain, so agents are encouraged to share these good practices with consumers, real estate agents and others on an ongoing basis as appropriate. Of course, these tips will work best in concert with appropriate technological security features including email encryption, spam filters, anti-virus, network protection, etc.

Examples of good business practices include:

- Exercise extreme caution when weighing any request to change wire instructions. Encourage all parties to do the same (Special Alert 15-07).
- Be wary of any email, phone call or other communication that involves threats, high pressure language or warns of "dire consequences" if immediate action isn't taken (Special Alerts 15-07 and 15-08).
- Be wary of emails with missing or unusual subject lines.
- Check emails to ensure the sender's address has not been altered. Fraudsters typically use email addresses that closely resemble a seller's (or any party's) actual email address (Special Alerts 15-08 and 16-01).
- Be wary of emails that include poor spelling or grammar, are over formal or that are written in a style uncharacteristic of the purported sender. Also, beware of emails that misuse industry terminology, for instance, references to the "HUD" instead of the "Closing Disclosure" (Special Alert 15-08).
- Be wary of any unexpected emails or requests, including internal requests purportedly from executives or others (Special Alert 15-07).
- Be wary of emails sent at odd hours (Special Alert 15-08).
- Be wary of any communication seeking to confirm information the purported sender should already have.
- Do not open unknown or unverified hyperlinks or downloads. Tip: Hovering your mouse over the sender's email address may reveal a different email address (Special Alert 15-08). Caution: Do not hover over unknown links within the body of a suspect email. Security experts formerly

recommended hovering as a way to determine the validity of such links. However, newer strains of malware may infect a computer when the user merely hovers over the link.

- Delete unsolicited emails from unknown sources.
- In the case of an invoice, verify any changes in vendor payment location and confirm requests for transfer of funds (Special Alert 15-07).
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via a personal email address, it's best to verify the legitimacy of the request via other channels.

RESPOND

What do I do if I spot attempted social engineering and wire fraud?

SUSPECT COMMUNICATIONS

What can agents and their staff members do if they receive an email, phone call or other communication that just doesn't feel right? Here are some suggestions we've discussed in the past (Special Alert 15-08):

- **GO WITH YOUR GUT:** Agents and staff should always be empowered to pause the process if they have any suspicion of fraud.
- **DO NOT GIVE IN TO PRESSURE:** Staff members who feel threatened or pressured by any communication should treat this as a red flag and immediately escalate the situation to management.
- **DON'T TRUST — VERIFY:** Verify via telephone the legitimacy of any wire instruction, or any suspect communication. Encourage all parties to the transaction to do the same.
- **DON'T CLICK:** Do not open or hover your cursor over unknown or unverified hyperlinks.

It's worth noting that staff members should use extraordinary care to not mention the words "fraud," "forgery" or similar words of suspected wrong-doing when verifying information. Further investigation and information gathering must be made by agency management before any action is taken. Suspicions of fraud and forgery should not be communicated to any other party without prior approval of management or a supervisor. Failure to take these precautions could result in a defamation suit if suspicions are unfounded (see Crime Watch Program Outline).

DIVERSION OF ESCROW FUNDS

We hope that funds are never misdirected by a fraudster. However, even the best-prepared companies in the world fall victim to fraud, so we can expect agents and underwriters to fall victim as well. We recommend agents create an Immediate Response Plan for the minutes and hours after discovering a diversion of funds. Agents who have had such plans have often been able to recover some or all of the funds diverted by fraudsters, although recovery may take time. Additionally, under the Uniform Commercial Code (UCC), a commercial customer of a bank has until midnight the next banking day to

report anomalies in their account indicating fraud. Once the deadline has passed, it becomes more difficult for the commercial account holder to rely on the bank for recovery. The most successful Immediate Response Plans are those established well in advance and communicated to staff members and the agency's bank. Plans will vary, but may reflect the following, as appropriate:

- **Minutes count:** Staff members should notify management the moment suspicion arises that a wire may have been misdirected. In today's electronic transfer system, funds can be moved in minutes after receipt. A swift response is critical to stopping the fraud.
- **Your relationship with your bank is critical:** When funds are diverted, your bank may be your first and best hope of either stopping or reversing the wire. Agencies that have established a close relationship with their bank and that continually dialog with the bank regarding fraud threats have a better chance of recovering funds. Some agents work with their banks to discuss wire retrieval scenarios and establish emergency contacts, often in the bank's fraud department, whom they can call at a moment's notice day or night.
- **Freeze the funds:** An agent's bank can be an important advocate with the receiving bank in a wire transfer. If funds have been transferred to the receiving bank and cannot be recalled, ask your bank (the sending bank) to formally request that the receiving bank freeze the funds. Some agents also have had success freezing funds by directly contacting the receiving bank.
- **Contact local law enforcement:** Contact local police in your jurisdiction and the jurisdiction of the receiving bank.
- **Contact your local FBI office:** The FBI, working with the U.S. Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds. Contact information for local FBI field offices is available at www.fbi.gov/contact-us/field-offices.

Following these initial steps, evaluate the following steps:

- Contact the underwriter involved in the transaction. Alliant National always is available to help you evaluate the situation.
- Contact your corporate attorney to let him or her know about the events taking place.
- Depending on the nature of the fraud, contact the appropriate insurance provider (Cyber-Liability, Escrow Security Bond or Errors & Omissions).
- File a complaint with IC3. For details on filing a complaint, visit bec.ic3.gov.

Quickly create a contact sheet for your Immediate Response Plan.
Download an editable PDF here.

RECOVER

How do I recover if my agency falls victim to wire fraud?

No one wants to find themselves in a position where they must recover from a loss due to fraud, yet the best companies in the world may be breached. We recommend having a solid "backstop" to protect your assets and your livelihood. Businesses that do not have a plan in place to recover from losses risk their survival. Have a Disaster Recovery Plan that includes appropriate insurance coverages as a "backstop" in the event a major fraud is successful. The three types of coverage that create a strong back stop are E&O, Escrow Security Bonds (ESBs) and Cyber-Liability policies. In some cases, none of these coverages will protect against social engineering unless a specific endorsement/rider is purchased. Business insurance can be complicated. Policies, programs and carriers should be carefully weighed to ensure appropriate coverage, and when it comes to social engineering fraud, some agents may be surprised to know their current plans no longer cover this risk. If you do have a policy, make sure that you notify the carrier within the required time frame, providing all required information with the notification of claim.

To help our agents, we have worked with our partners at Thompson Flanagan, insurance brokers based in Chicago, to develop an insurance program including an ESB, a Cyber-Liability policy and E&O coverage tailored to title agencies. You can purchase them as a package or separately. The purpose of this program is to provide an option designed for title agents. Social engineering fraud losses generally are not covered by E&O policies, Fidelity Bonds or even Cyber-Liability insurance. Cyber-Liability insurance may cover the agent for losses if its systems are hacked, or it may cover expenses around breach notification and credit monitoring if consumer data is compromised. However, social engineering schemes generally fall outside the scope of this coverage. Many underwriters now offer a social engineering endorsement, or rider, to protect agents from the risks posed by this type of fraud. According to Thompson Flanagan, social engineering endorsements for title insurance agents commonly are sub-limited to $250,000. For instance, if you have an ESB with $1 million of coverage with an endorsement for social engineering, the endorsement might be limited to a maximum of $250,000. Agents can expect to pay a 10 percent or 20 percent additional premium charge for such coverage. However, Thompson Flanagan may be able to include a social engineering endorsement with your ESB coverage at no additional cost.

Applying for the coverage is the best way to understand the options available to your company. Thompson Flanagan has a program specifically designed for our agents, and their application is very straightforward.

Thompson Flanagan Alliant National Agents Title Insurance Coverage Agent Application

If you have specific questions about the policies they offer, please feel free to contact them directly:

Julio Bermudez, Senior Vice President: jbermudez@thompsonflanagan.com p: (312) 239-2881

Michael Cermak, Broker: mcermak@thompsonflanagan.com p: (312) 239-2893

APPENDIX: RESOURCES

Share these materials with your team

ESCROW FRAUD/SOCIAL ENGINEERING

ALLIANT NATIONAL

BEC/EAC BY THE NUMBERS

Email and wire fraud attacks on title agents are part of a growing fraud threat targeting businesses of all sizes and the general public. This threat is known as **Business Email Compromise/Email Account Compromise (BEC/EAC).**

103 COUNTRIES & ASIAN BANKS

Fraudulent transfers have been sent to 103 countries. Most have gone to banks located in China and Hong Kong.

ALL 50 STATES &131 COUNTRIES

BEC/EAC scams have been reported in all 50 states and in 131 countries.

$1.59 BILLION 22,000 U.S. VICTIMS

Fraudsters stole or attempted to steal more than $1.59 billion from roughly 22,000 U.S. victims between October 2013 and December 2016.

COMPLAINTS UP 480%

Complaints from title companies targeted by BEC/EAC scams rose 480 percent in 2016.

BEC/EAC IN THE TITLE INDUSTRY

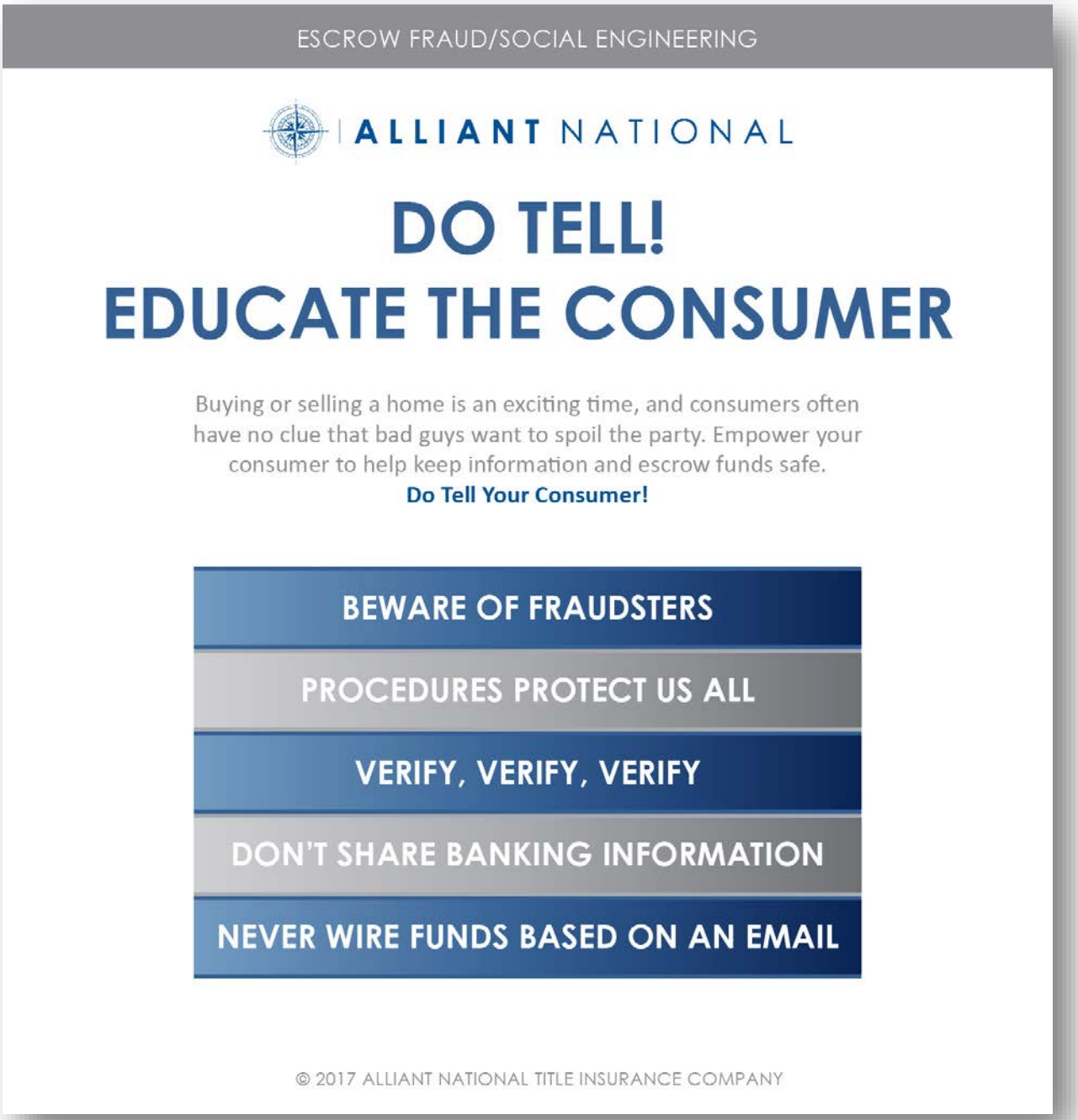
Overwhelmingly these scams involve attempts to divert wires. However, the FBI warns that BEC/EAC scammers increasingly are targeting organizations with the primary goal of obtaining personally identifiable information (PII) or wage and tax statement (W-2) forms for employees.

** Data from the FBI's Internet Crime Complaint Center (IC3)*

Download at:

http://arc.alliantnational.com/Libraries/Fraud_Education/BEC_EAC_Infographic_11_6_17_V1.sflb.ashx

Download at:
http://arc.alliantnational.com/Libraries/Fraud_Education/7_Deadly_Scams_Infographic_11_3_17_V2.sflb.ashx



Download at:

http://arc.alliantnational.com/Libraries/Fraud_Education/Do_Tell_Infographic_11_3_17_V1.sflb.ashx

Download at:
http://arc.alliantnational.com/Libraries/Fraud_Education/WTDFR_Infographic_11_3_17_V1_copy.sflb.ashx

ALLIANT NATIONAL TITLE INSURANCE COMPANY

IMMEDIATE RESPONSE PLAN: WIRE FRAUD CONTACTS

Keep this sheet near your phone

IF A WIRE IS DIVERTED:

1. **Contact Your Bank**

   First, ask your bank (sending bank) to stop the transfer or recall the funds. Some agents also have had success freezing funds by directly contacting the receiving bank. If funds have been transferred to the receiving bank and cannot be recalled, ask your bank to formally request that the receiving bank freeze the funds. Make sure to specify that fraud is suspected.

   Your (sending) Bank Name: _____ Fraud Dept. Main Number: _____

   24 Hour Fraud Dept. Contact Name & Number

   Contact 1 Name: _____ Phone Number: _____

   Contact 2 Name: _____ Phone Number: _____

2. **Contact Local Law Enforcement**

   Contact local police in your jurisdiction, and the jurisdiction of the receiving bank.

   Local Police Department: _____ Financial Crimes Division: *(if applicable)*

   Main Number: _____ Contact Name: _____

   Phone Number: _____

3. **Contact the Local FBI Office**

   The FBI, working with the U.S. Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds. Contact information for local FBI field offices is available at https://www.fbi.gov/contact-us/field-offices.

   FBI Office City: _____ Phone Number: _____

Following these initial steps, evaluate the following steps:

4. **Contact the Underwriter Involved in the Transaction**

   Alliant National always is available to help you evaluate the situation.

   Alliant National Regional Agency Manager

   Name: _____ Phone Number: _____

   Note: If the insured under the policy is a potential victim of fraud, please contact the Alliant National Claims Department at 877-788-9800, ext. 425, or submit a claim to Alliant National at claims@alliantnational.com. Directions for submitting a claim can be found at www.alliantnational.com/claims/howtosubmitaclaim.

Download at:

http://arc.alliantnational.com/Libraries/Fraud_Education/Immediate_Response_Plan_contact_sheet_rev_7_11_28_2017.sflb.ashx

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

5. **Contact Your Corporate Attorney**
   Attorney Name: _____ Attorney Number: _____

6. **Contact Your Insurance Provider**
   Depending on the nature of the fraud, contact the appropriate insurance provider (Cyber-Liability, Escrow Security Bond or Errors & Omissions).
   Insurance Carrier 1: _____ Coverage: _____
   Contact Name: _____ Phone Number: _____

   Insurance Carrier 2: _____ Coverage: _____
   Contact Name: _____ Phone Number: _____

   Insurance Carrier 3: _____ Coverage: _____
   Contact Name: _____ Phone Number: _____

7. **Contact Your Regulator (if applicable and/or required by law):** In certain jurisdictions, an agent may be required to notify their title or escrow licensing agency.
   Regulator: _____
   Contact Name: _____ Phone Number: _____

8. **File a Complaint with the FBI's Internet Crime Complaint Center (IC3)**: For details on filing a complaint, visit https://bec.ic3.gov/.

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

1831 Lefthand Circle, Suite G | Longmont, CO 80501 | 1-877-788-9800
AlliantNational.com

Disclaimer: These materials do not constitute legal advice. These materials are for informational purposes only.