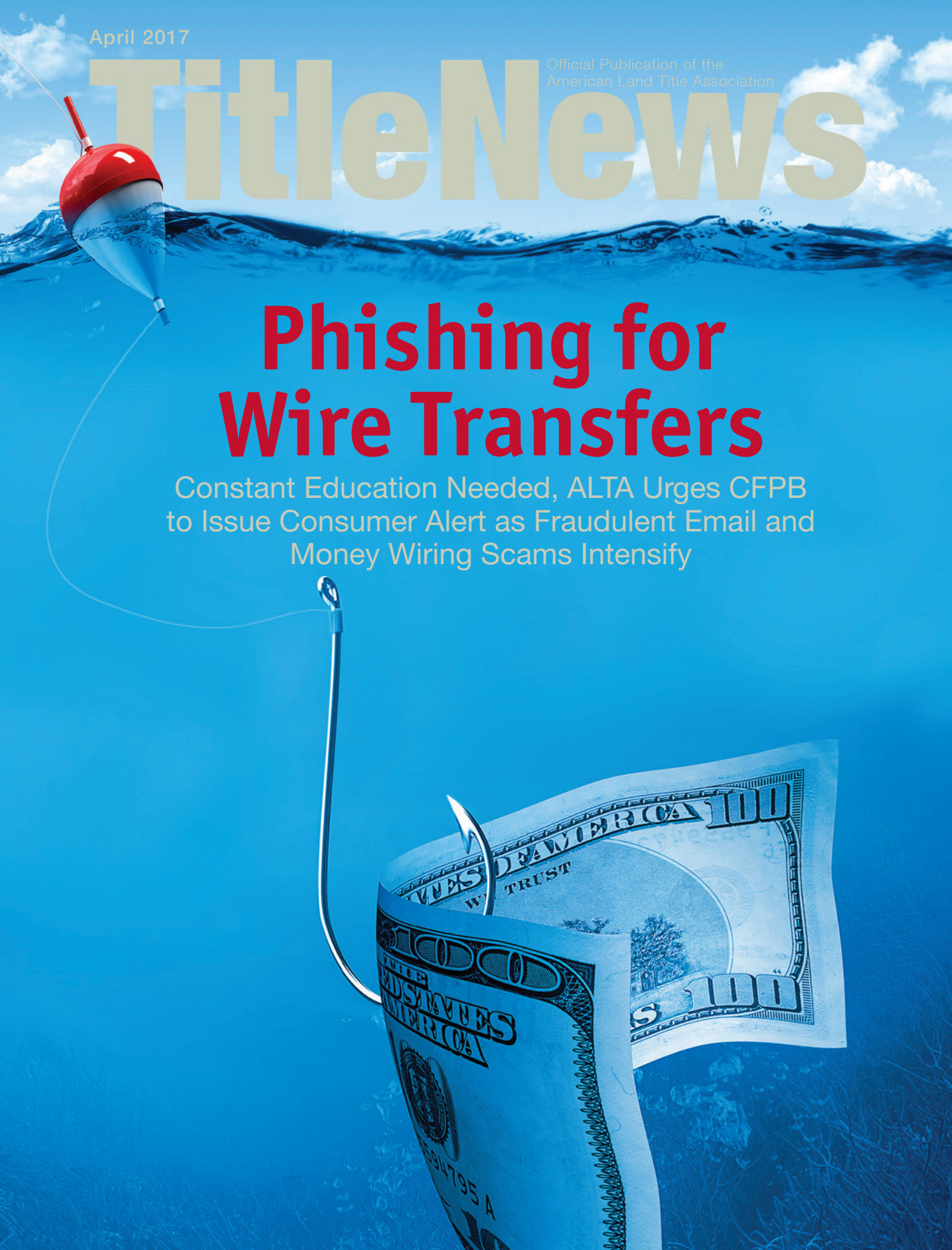
April 2017

TitleNews

Official Publication of the
American Land Title Association

Phishing for Wire Transfers

Constant Education Needed, ALTA Urges CFPB to Issue Consumer Alert as Fraudulent Email and Money Wiring Scams Intensify



Phishing for Wire Transfers

Constant Education Needed, ALTA Urges CFPB to Issue Consumer Alert as Fraudulent Email and Money Wiring Scams Intensify

As president and chief executive officer of Texas-based Rattikin Title Company, Jack Rattikin III has plenty of things that occupy his attention. Third-party vendor oversight and threats to the rating structure in Texas are two top-of-mind issues, but they're not what keeps Rattikin up at night. Over the past year, a new threat has emerged to become the main reason for late-night tossing and turning for title and settlement professionals: phishing and wire fraud.

"I make it clear in every staff meeting and with our closing teams that wire fraud is our number one concern," Rattikin said. "It's not just closing deals and searching titles anymore. There's a lot of risk that we have to think about every day. This is what keeps me up at night. A large wire that ends up in Russia or China could put us out of business." >>

By Jeremy Yohe


100
100
100

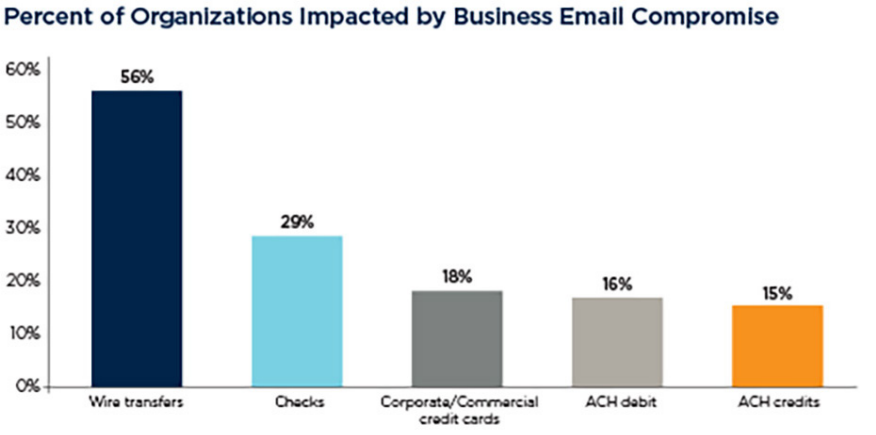
How It Starts

Criminals begin the wire fraud process way before the attempted theft occurs. Most often, they begin with a common social engineering technique called phishing. This can take the form of email messages, website forms or phone calls to fraudulently obtain private information. Through seemingly innocuous communication, criminals trick users into inputting their information or clicking a link that allows hackers to steal login and password information.

Phishing emails might appear to come from a legitimate business or recognized user. Spear phishing is a more targeted email attack sent to a select number of users, while a whaling attack, also known as Business Email Compromise (BEC), is a more targeted variation of spear phishing aimed at high-profile executives or personnel who manage wire transfers. According to the latest Association for Financial Professionals' Payments Fraud and Control Survey, a majority of finance professionals (64 percent) reports that their organizations were exposed to BEC in 2015. The FBI's Internet Crime Complaint Center reports that "the BEC scam continues to grow, evolve and target businesses of all sizes." Since January 2015, there has been a 1,300 percent increase in identified losses, now totaling over $3 billion.

The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone. Don't rely on email alone.

Martin Licciardo, a special agent in the FBI's Washington Field Office, said the best way to avoid getting ripped off is to verify the authenticity of requests by speaking to people directly.



Source: Association for Financial Professionals

"The ability of these criminal groups to compromise legitimate business e-mail accounts is staggering," he said. "They are experts at deception."

It is disconcerting that, in spite of safeguards being implemented, criminals are still making headway with BEC scams. The significant increase in wire fraud also suggests that BEC fraud may be more difficult to prevent than was previously believed.

Once hackers gain access to an email account, they will monitor messages to find someone in the process of buying a home. Hacks can come from various parties involved in a transaction, including real estate agents, title companies, attorneys or consumers. Criminals then use the stolen information to email fraudulent wire transfer instructions dressed up to appear as if they came from the victim. To this end, criminals will use either the victim's actual email account (which they may actually control) or create a fake email account resembling the victim's email.

"We all want to avoid the scenario where the buyer's funds are sent to a fake account and are unrecoverable," said Bill Burding, a member of ALTA's Information Security Committee and general counsel for Orange Coast Title Co. "One of the key indications of any wire fraud scam is the sense of urgency. These tend to come from someone of authority to the person who is responsible for wiring funds within the organization. This is when it's imperative to slow down and make sure policies for handling wire instructions are followed to a T."

Over the past few years, there's been a lot of discussion and training over the past few years about preventing outbound wires from being intercepted. According to Christopher Hacker, chief product officer at ShortTrack, criminals are now targeting the "inbound wire" of cash to close sent by the buyer..

"Unfortunately, again and again, we hear leaders of title agencies say they're handling all of the wire diversion and fraud issues with the controls for outbound wires," Hacker said. "The bad actor sits and waits for the wire instructions to show up in the buyer's inbox, downloads them, deletes the message with the accurate document and resends updated wire instructions either from a spoofed account of the title company or from

the compromised account of the real estate agent."

ALTA Urges CFPB to Issue Alert

ALTA encourages the Consumer Financial Protection Bureau (CFPB) to publish a consumer alert warning consumers about these schemes. In the letter, ALTA informed CFPB Director Richard Cordray that criminals frequently target homebuyers prior to title companies getting involved in transactions. With the spring homebuying season underway, ALTA believes the alert should give consumers tips on how to protect their money and information, providing questions to ask real estate professionals to determine if they have adequate procedures in place to protect transactions.

Other regulators already have issued warnings. In February, the Missouri Department of Insurance (DOI) followed the Colorado Division of Real Estate at the Department of Regulatory Agencies, the Federal Trade Commission and the Financial Crimes Enforcement Network (FinCEN) in issuing warnings about fraudulent email and money wiring scams.

Following several investigations related to fraudulent email schemes during real estate transactions, the Missouri DOI reported that emails were received in each instance changing the original instructions for disbursement of funds previously provided by a consumer. The Colorado regulator encouraged title professionals to implement procedures to "verify and call back" to the consumer, ensuring the instructions are correct.

"To prevent these schemes, underwriters, title agencies and attorneys should educate their staff about fraudulent emails and implement procedures for handling wire instructions," said Frank Pellegrini, a member of ALTA's Information Security Committee and president of Prairie Title Services.

"Not only must you train your staff, but everyone involved in real estate transactions must also be aware of the potential losses from criminals phishing for information, stalking

Examples of Fraudulent Emails

Here are a couple of examples of the type of email you may receive.

Sometimes the email address looks correct, but the "reply-to," which isn't displayed in most email programs, can be masked or undisclosed, and can lead to unfamiliar or personal email domains. Note the use of the gmx.com domain, which is notorious in this type of scheme.

```
From: [Name] <[actual email address]>
To: Details
Hello,
Please I need you to do a quick wire transfer to a
local bank for me. Get back at me with the info you
need to do the wire transfer.
```

Here's an example of a spoofed inter-office email attempting to get an employee to change wiring information.

```
From: [Name] <[name]@gmx.com>
To: [Internal Employee email]
Subject: Urgent – proceeds
[First Name],
Seller wants proceeds wired to their trading account
how can you help?
```

In this example, the agent had an email address that incorporated the company domain, but the "from" was a Gmail address designed to make the recipient think it was a legitimate correspondence. In addition, two digits of the phone number in the email signature line were transposed.

```
From: [Agent Name] <[agent-name]@gmail.com>
To: [Client]
Subject: Urgent – regarding [Listing Address]
[First Name],
To move forward on [address] we need to have the money
wired immediately. Once you wire [amount] to [wiring
instructions] I will call you. I am in a meeting and
will not be available to talk until I call you later.
```

closings and hoping someone makes a mistake."

In addition to training, companies need to enhance computer security while also following sound policies and procedures to reduce risk. Like many companies, Rattikin Title has a dual verification policy for any wire transfer—any wire initiated by a closer must be verified by another escrow officer.

"We try to get wire instructions from the seller and payoff lender as early as possible in the transaction and won't accept any changes," Rattikin said. "We have a statement in our wire instructions that says they will never change. So, if someone receives communication from us that says it changed, they know it wasn't from us."

Many times, the fraudulent emails involve wires asking for less than $100,000 so the transactions don't attract the FBI's attention. Rattikin says his company forwards every suspect wire transfer request to the FBI.

"The closing staff gets bombarded with business toward the end of the month and is extremely busy," Rattikin said. "The problem is that the fraudsters know that. They know it's a likely time your closers may make a mistake."

Sample Warnings

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

- put consumer warnings on websites and communications
- 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.

Red Flags

Title and settlement companies can protect themselves by increasing staff awareness of these scams. According to the FBI, businesses that deploy robust internal prevention techniques at all levels (especially training front-line employees who may be targeted by initial phishing attempts), have proven highly successful in recognizing and deflecting email scam attempts. Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of those requests. Here are some red flags:

- A customer's seemingly legitimate emailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.
- Transaction instructions originate from an email account closely resembling a known customer's email account; however, the email address has been slightly altered by adding, changing, or deleting one or more characters. For example:
  - Legitimate email address: *john-doe@abc.com*
  - Fraudulent email addresses: *john_doe@abc.com* or *john-doe@bcd.com*
- Emailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
- Emailed transaction instructions direct wire transfers to a foreign bank account that has been documented in customer complaints as the destination of fraudulent transactions.
- Emailed transaction instructions direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- Emailed transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret," or "Confidential."
- Emailed transaction instructions are delivered in a way that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- Emailed transaction instructions originate from a customer's employee who is a newly authorized person on the account or is an authorized person who has not previously sent wire transfer instructions.
- A customer's employee or representative emails a financial institution transaction instructions on behalf of the customer that are based exclusively on email communications originating from executives, attorneys or their designees. However, the customer's employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys or designees.
- A customer emails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- A wire transfer is received for credit into an account, however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor, while thinking the new account belongs to the known supplier/vendor. This red flag may be seen by financial institutions receiving wire transfers sent by another financial institution as the result

of email-compromise fraud.

ALTA's Title Insurance and Settlement Company Best Practices details policies and procedures title and settlement companies should follow to protect money and non-public personal information (NPI).

important point is to remind your customers that legitimate businesses like yours would never solicit sensitive personal information through insecure channels like email or text messages.

> "We receive these emails several times a month. Make sure your employees ask questions. There are no stupid questions when it involves money."

What If You Get Phished?

According to the FTC, companies impersonated as part of an email phishing scam should notify customers as soon as possible, contact law enforcement, provide resources for affected consumers and review their own security practices. Offering immediate advice and support can help companies retain customer goodwill. Here are tips on how to respond if your business is impersonated in a phishing scam:

- **Notify consumers of the scam.** If you are alerted to a phishing scam in which fraudsters are impersonating your business, inform your customers as soon as possible. If your business has a social media presence, announce the scam on your social media sites and warn customers to ignore suspicious emails or texts purporting to be from your company. You can also inform your customers of the phishing scam by email or letter. The
- **Contact law enforcement.** If you become aware that criminals are impersonating your business, report the scam to the FBI's Internet Crime Complaint Center (*www.ic3.gov*). Suggest that affected customers forward any phishing emails impersonating your business to the Anti Phishing Working Group (*www.antiphishing.org*), a public-private partnership against cybercrime.
- **Provide resources for affected consumers.** If consumers believe they may be victims of identity theft because of a phishing scam, direct them to *www.identitytheft.gov*, where they can report and get resources to help them recover from identity theft. For more information about recommended computer security practices, direct consumers to resources on the FTC's consumer information site, where they can learn how to protect themselves online and avoid future phishing attacks.

Education Essential

Gregory McDonald, chief executive officer of Cloudstar Corp., said educating all parties involved in the transaction is vital, and keeping wiring instructions on paper is the best solution.

"Title companies should talk to their customers after a deal comes in, and during the process, and let them know that nobody will email changes to wiring instructions," McDonald said. "This is a human problem that cannot be resolved by technology. No fancy lock—no matter how high tech—will stop a thief that identifies themselves as a police officer when knocking on your front door."

Companies should use fraudulent emails as a reminder to update security practices and as a staff training opportunity. Criminal organizations that perpetrate these frauds are continually honing their techniques to exploit unsuspecting victims, which makes constant awareness and education a necessity.

"Data security isn't just a one-and-done checklist as threats are ever-evolving, so defenses need to be nimble," Rattikin said. "My company has yet to lose any money due to wire fraud—knock on wood—but we receive these wire fraud attempts several times a month. Make sure your employees ask questions. There are no stupid questions when it involves money."

Jeremy Yohe is vice president of communications for ALTA. He can be reached at jyohe@alta.org.