Investors Title
INNOVATIVE BY INSTINCT

FRAUD ALERT

Fraudulent Payoff Statement Results in Big Losses
Online Fax Account Compromised
Increase Your Password Security

In our ongoing efforts to keep approved providers, agents, and other partners informed of potential threats to their business, we distribute fraud alerts so that you are aware of potential threats and can take the necessary steps to guard against them.

We have distributed numerous alerts, newsletters, and other communications regarding the epidemic of wire fraud in our industry. While we know that you are actively combatting this ever-growing problem, the fraudsters' techniques have continued to evolve in response to the industry's diligent efforts to frustrate their schemes.

A North Carolina real estate attorney recently reported being the victim of a social engineering scam that involved the compromise of an online third-party service provider and a fraudulent payoff statement. This scam resulted in the settlement provider being tricked into wiring a very large payoff to the fraudster's bank account. This scam could be perpetrated on any settlement provider.

The Fraudulent Fax Payoff Scam

While we have all been previously alerted to the compromises of "free" and "online" email providers, this particular scam involved an online fax service that delivers emails into a user's email account. This type of service may be useful to deliver faxes to your email inbox such that they may be retrieved on the computer or on the phone. In this instance, convenience came with a large cost. Here is how the fraudster did it:

1) The fraudster gained access to a settlement provider's online fax account by learning the login and password.
2) The fraudster monitored the online fax account by substituting another email address to intercept every fax. (The fraudster's email account happened to be a hard-to-trace "free" email account.)
3) After reviewing the faxes, the fraudster forwarded them to the settlement provider at the settlement provider's correct email address.
4) When the fraudster saw a payoff statement, they altered the payoff with new wiring instructions and forwarded the altered fraudulent payoff statement to the settlement provider.
5) The settlement provider wired the payoff to the fraudster's account.

But I Thought . . .

1) ***Isn't a fax safer than email?*** Anyone can buy a fax machine and send a spoofed fax. This scenario could actually happen before email existed, and now multiple apps exist allowing users to send spoofed faxes from their computers or mobile devices. What the settlement provider did not consider was that when a fax arrives as email, it is email. Always confirm wiring instructions before sending a wire.

2) ***What if my faxes are sent through encrypted email?*** While you should choose an online fax service that provides for encryption of these communications to your email inbox, this particular fraudulent scheme would not have been avoided if encryption had been used. The problem was in the apparent compromise of the login credentials and password.

What could have been done differently to stop this fraud?

1) **Password Policies:** Password policies should be in place to deter this type of fraud scheme. To be compliant with ALTA Best Practices, passwords should be:
   - Minimum of eight characters in length (many security experts are recommending 12-16)
   - Complex - requiring letters, numbers, uppercase, lowercase, and special characters
   - Changed frequently – at least every three months
   - Unique to the user (i.e., no sharing of passwords)
   - Unique to the service
     - DO NOT use the same password for multiple services (e.g. for the bank, for email, for online faxes, or for access to your server). If a fraudster finds out one password, you do not want them to be able access everything. You should compartmentalize your cyber-fraud risk.

   Your password policy should apply to every single system that you access. This risk of a compromise exists for your email, phone, server, online banking, online fax service, online backup service, online loan package retrieval, social media -- anything with a password. If you have made the mistake of reusing your password on multiple platforms, you run the risk that when one password (and therefore system) is compromised that all of your systems will be compromised.

   - If you have not changed your passwords lately (on all systems), do so now.
   - While logged in to your online accounts, confirm your profile settings (paying close attention to contact information and email addresses).

2) **Wiring Procedures:** Procedures should be in place to require verbal confirmation of wiring instructions with a verified source. We have prepared materials to assist you in developing a compliant and effective procedure.

   W.I.R.E. – **W**hat **I** **R**equire **E**very time (Click Here) includes steps, policies, and procedures to consider ***before*** you send another wire out of your office.

3) **Information Security Policy:** A policy should be in place to protect your and your clients' money and sensitive information. We have prepared materials to assist you in developing compliant and effective procedures:

   C.Y.B.E.R. – **C**an **Y**ou **B**e **E**ntirely **R**eady (Click Here) includes steps, policies, and procedures to consider in formulating your Information Security and Trust Account Security Plans.

4) **Cyber Fraud Response Plan:** A plan should be in place before you fall victim to a fraud scheme. We have prepared materials to assist you in developing a compliant and effective procedure:

   F.A.S.T. – **F**ast **A**ction **S**tops **T**heft (Click Here) includes steps, policies, and procedures to consider in formulating your Cyber Fraud Response Team and your Cyber Fraud Response Plan.

5) **Spread the Word about Cyber Fraud:** We have prepared consumer and client materials to assist with this process and they are located at https://invtitle.com/fraud.

6) **Get Cyber Fraud Insurance:** Contact your insurance agent to inquire about getting cyber fraud insurance to cover all three of the following:
   - Cyber Breach (Loss of Data)
   - Cyber Theft or Cyber Crime (Loss of Money)
   - Social Engineering (Tricked into sending wire to wrong account)

We also have a separate article that details these different types of coverages. Click here for that article. You can find names of cyber fraud insurance providers in our VIP program at http://invtitle.com/vip

---

We are interested in alerting approved providers, agents, and other partners in the real estate business of any and all external and internal threats and fraud scams. In the event that you become the target of a fraud scam, please share that experience with us so that we may alert others. You may email the facts about the attempted fraud scam to riskmanagement@invtitle.com.

This fraud alert is a service of Investors Title. If you have any questions about this alert, please feel free to contact Jonathan Biggs, vice president of risk management and education at riskmanagement@invtitle.com.

Investors Title | 121 N. Columbia Street, Chapel Hill, NC 27514 | 800.326.4842
invtitle.com