SHINE BRIGHT
January 2020

FRAUD ALERT: OUTWITTING PHONE SCAMMERS

It's a sorry day when we can't even count on our phones to tell the truth. But new applications like SpoofCard, which gives criminals a way to change what someone sees on their caller ID display, present the newest nightmare for the title and, by extension, real estate industries.

To spoof a call, a cyber thief need only dial one of SpoofCard's access numbers and enter the phone number they want to target followed by the number they want to appear on the recipient's caller ID.

"In other words," said Thomas Cronkright, chief executive officer of CertifiD, "the recipient of a call thought to be coming from one person is actually coming from someone else. Even trained professionals can fall victim."

As an example, a hacker could 'spoof' a title company and call the buyer when it's time to wire closing funds. Or they could impersonate a seller, call the title company, and provide fraudulent wiring information for net proceeds to be transferred after closing.

"It's important for real estate professionals as well as title and settlement agents to adopt safety techniques to mitigate instances of fraud," Cronkright said.

This includes giving buyers and sellers strict instructions not to respond to last-minute requests for changes in their wiring instructions. At minimum, in such instances, it should mandate a call back to a number they know is legitimate - such as the real estate or title agent they've been dealing with - and speaking live with the person whose voice you know.

The American Land Title Association (ALTA) reports that imposters made more than 250,000 spoofed phone calls last year, according to the Federal Trade Commission - and FBI data shows that $969 million was "diverted or attempted to be diverted" from real estate purchase transactions and wired to criminally controlled accounts during fiscal year 2017.

What can real estate, title and escrow professionals do?

"The key is in early training and education of all transaction participants on how wiring information will be exchanged," said Cronkright, "so that people can identify a fraudster before it's too late."

Companies need to take a step back, he added, to review how they exchange and confirm wiring information and identify areas where someone could pierce through the communication chain and expose someone to loss.

We can't always rely on phone calls any longer.

Powered by **Title Resources**
www.TitleResources.com