https://www.wsj.com/articles/hackers-defraud-homeowners-out-of-hundreds-of-thousands-of-dollars-11563528600

PRO CYBER NEWS

Hackers Defraud Homeowners Out of Hundreds of Thousands of Dollars

Cybercriminals increasingly target real-estate deals, breaking into email accounts to craft custom scams

The New Jersey house sold by Robert Masucci and Clare Falbe Masucci. PHOTO: ROBERT MASUCCI

By Adam Janofsky

Updated July 19, 2019 8:46 am ET

Last August, Robert Masucci and Clare Falbe Masucci sold their house in Glen Ridge, N.J., for about $840,000 after owning it for 30 years.

About an hour after the transaction closed and the profits from the sale arrived in their bank account, their lawyer received an email purporting to be from Mr. Masucci, instructing the lawyer to send the payout somewhere else.

After calling Mr. Masucci, the lawyer realized it was a scam—but the couple's troubles weren't over.

About three weeks later, New Jersey community lender Gibraltar Bank sent them a notice saying their latest mortgage payment hadn't been received. The Masuccis thought their mortgage had been paid off immediately after the house was sold. It turned out the funds earmarked for Gibraltar Bank had gone astray.

Cybercriminals are increasingly targeting real-estate professionals, title agents and lawyers involved in buying and selling homes. In many cases, hackers compromise the email account of one party and read through correspondence to craft custom scams, often stealing hundreds of thousands of dollars at a time. If the fraud isn't quickly discovered, funds can be difficult or impossible to recover, cybersecurity experts said.

Real-estate wire fraud hit 11,300 people in 2018, leading to more than $149 million in losses, according to data from the Federal Bureau of Investigation. That was up from 9,645 victims in 2017 who lost more than $56 million.

"It's been an absolute epidemic. No company, large or small, is immune, and neither are individuals," said Melissa Krasnow, a partner at VLP Law Group LLP who specializes in data security and privacy. Large corporate data breaches could give cybercriminals more data to run targeted scams, she said.

The Masuccis eventually learned that before the sale closed, their lawyer had forwarded the title company bogus mortgage payout instructions contained in a separate email, apparently sent by a hacker aiming to siphon money from the real-estate deal. On the day of the close, the title company transferred about $180,000, funds intended to pay off the mortgage, to the hacker's bank account, said Gibraltar Bank Chief Financial Officer Linda Mourao.

"The money never got to us," Ms. Mourao said. "The title company should have known it was the wrong account."

"By the time we realized what happened, the money was long gone and the [hacker's] account was closed," Mr. Masucci said. "We were on the hook for $180,000."

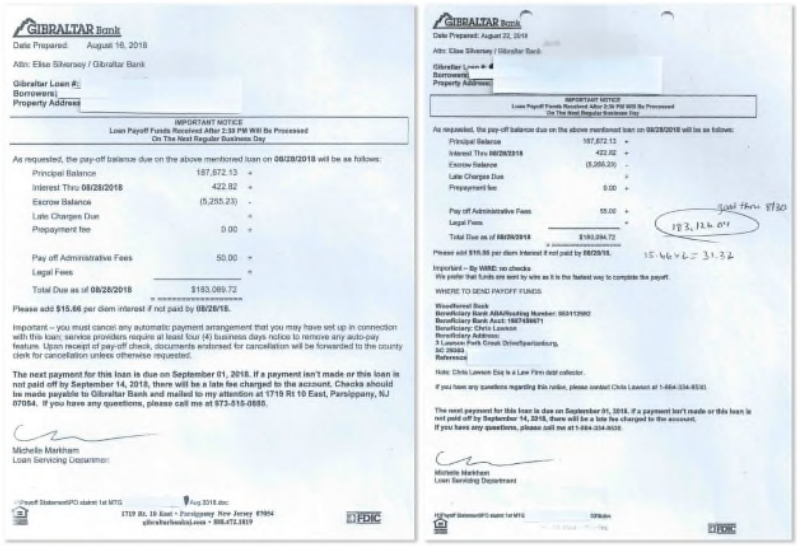
Mr. Masucci said seven months of negotiations resulted in the title company agreeing to pay off the couple's mortgage. The hacker was never caught. The Masuccis' lawyer and title company couldn't immediately be reached for comment.

Businesses have also been victims of real-estate fraud. Thomas Cronkright, chief executive of Sun Title Agency LLC in Grand Rapids, Mich., said his company was scammed out of $180,000 during the 2015 sale of a gas station. The company recovered most of the money after working with law enforcement for two years, he said.

Mr. Cronkright has since co-founded CertifID LLC, a software company focused on preventing wire fraud in real-estate deals.

In June, 43 House lawmakers sent a letter to Federal Reserve Chairman Jerome Powell asking the central bank to explore policies to protect home buyers from wire fraud.

Separately, Sen. Doug Jones (D., Ala.) in June teamed up with the American Land Title



The Masuccis' real mortgage-payoff statement from Gibraltar Bank, left, and a fraudulent one, right. The fraudulent document specifies the funds should be sent by wire transfer, not by check, while the real document calls for a check.

Association and other real-estate industry groups to launch the Coalition to Stop Real Estate Wire Fraud. The group plans to educate home buyers about such scams, starting with residents of Pittsburgh; Virginia Beach, Va.; and Birmingham, Ala.—three cities that have seen large increases in first-time homeownership.

Mr. Jones said last month in a call with reporters that constituents in Alabama have been victims of such fraud, one losing $12,000 and another $250,000.

Real-estate agent Richard Hopen was caught up in an email scam when he sold his own house in 2017. Hackers got away with $239,000 in that transaction, he said.

He advocates laws to change the way wire transfers work.

One solution he favors is to require banks to make sure the name of the person or organization intended to receive a wire transfer matches the name on the bank account. A mismatch, he said, would stop a wire transfer.

The U.K. plans to require payment firms to do this starting next year. The House lawmakers cited the U.K. regulation in their letter to the Fed.

"Most real estate professionals know of the problem, but they don't understand how it occurs and how to prevent it," Mr. Hopen said.

Write to Adam Janofsky at adam.janofsky@wsj.com