OFFICE OF PRIVATE SECTOR
DIRECTOR'S OFFICE

Liaison Information Report (LIR)
Financial Sector

17 August 2017 LIR 170817001

E-mail Account Compromise Techniques Used to Steal Millions in Real Estate Settlement Funds

Handling Notice: Recipients are reminded the Office of Private Sector (OPS) LIRs contain sensitive information meant for use primarily within the corporate security community. FBI Headquarters Divisions and Field Offices may share LIRs with private sector partners they deem appropriate. Private sector partners shall not release these products in either written or oral form to the media, general public, or other personnel who do not have a valid need-to-know without prior approval from an authorized OPS official.

Overview

The Office of Private Sector, in coordination with the Criminal Investigative Division, is providing this LIR to inform private sector partners about the increasing use of e-mail account compromise[a] (EAC) techniques in the US real estate settlement industry. Consumer borrowers, settlement/title companies, real estate agents, real estate attorneys, builders, and others are being targeted by criminal actors netting millions in illicit proceeds. These proceeds are often directed initially to US banks then re-directed via money service businesses[b] and international accounts to Mexico, Nigeria, South Africa, China, Ghana, Turkey, and India. The increased use of EAC techniques, as well as, the evolving expansion into previously unidentified countries indicates this fraud scheme is not slowing and puts additional strain on industry participants to be vigilant with their e-mail communications and identity verification processes.

Criminal threat actors diverted an estimated $19 million in fiscal year 2016 from real estate purchase transactions by manipulating e-mail communications of key participants to re-direct legitimate wire transfers, including down payments, earnest money, and settlement proceeds to criminally-controlled accounts. The increasing use of EAC techniques such as identifying realtors via real estate web sites, spoofing, phishing, social engineering, chat rooms, spam, and malware is attributable to positive real estate market indicators such as housing prices/supply, interest rates, the increase in well-publicized multi-

[a] In e-mail compromise scams, criminal actors use social engineering or computer intrusion techniques to compromise the e-mail accounts of unsuspecting victims. In many cases, a criminal actor first gains access to a victim's legitimate e-mail address for reconnaissance purposes. The criminal then creates a spoofed e-mail account that closely resembles the legitimate account, but is slightly altered by adding, changing, or deleting a character. The spoofed e-mail address is designed to mimic the legitimate e-mail in a way that is not readily apparent to the targeted individual. The criminal actor then uses either the victim's legitimate e-mail or the spoofed e-mail address to initiate unauthorized wire transfers.

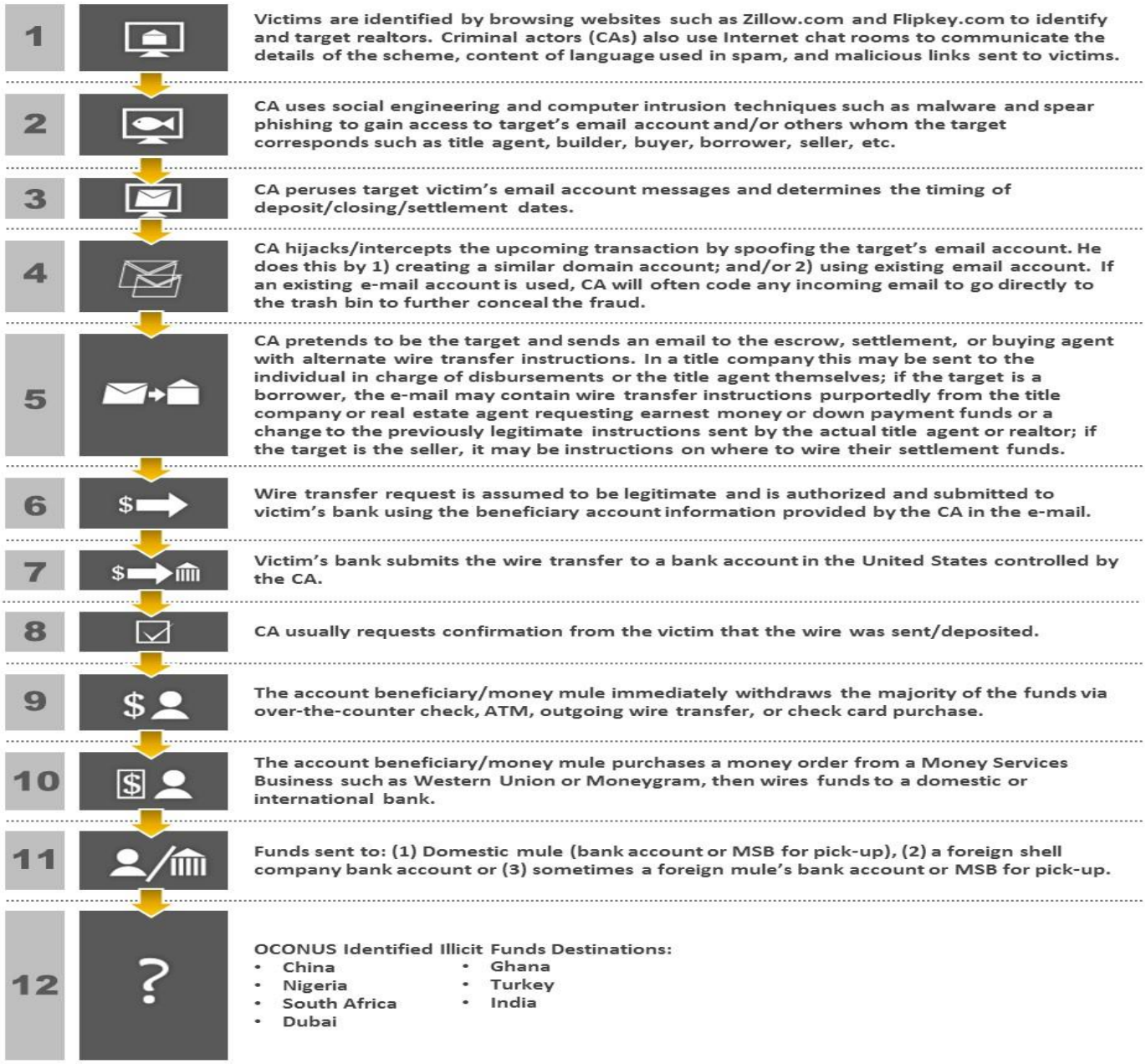
[b] The term money services business includes any person doing business, whether or not on a regular basis or as an organized business concern, in one of more of the following capacities: currency dealer or exchanger; check casher; issuer of traveler's checks, money orders or stored value; money transmitter; US Postal Service.

million dollar land development contracts, and the proven ease in infiltrating the transaction process. This threat will likely continue on an upward trend as these conditions persist. Please see the below diagram for a step by step overview of a common EAC scam.

(U) E-mail Account Compromise: Real Estate Settlement Industry – A Common Scheme Diagram

E-mail Account Spoofing Techniques

Using existing e-mail account: Actual sender is masked and does not appear in the "reply to" field, yet does appear in email header.
Adding/removing characters: From legitimate *widgets@freemail.com* to *widget@freemail.com*.
Rearranging characters: From *acme868@freemail.com* to *acme686@freemail.com*.
Replacing characters: In a sans serif font frequently used in e-mail to Arial, different characters appear to be similar: *sales@freemail.com* to *sales@freemail.com*; *sales@freemail.com* to *sales@freemail.com*.



UNCLASSIFIED

The FBI Perspective

One of the most widely reported vulnerabilities identified by victims is that industry participants in real estate settlements – whether they involve all-cash or mortgage loan purchase transactions – may not be aware of the minute differences or changes in the e-mail accounts of parties with whom they routinely conduct business. Consequently, they are inadvertently participating in the illicit transfer of funds to criminal actors. As real estate settlement transactions occur on a regular and recurring basis and typically use long-established straightforward processes between known participants (brokers, financial institutions, real estate agents, title and escrow companies and attorneys), it is very likely criminal actors and organized groups will increasingly continue to target these businesses and individuals for illicit financial gain.

- According to FBI information, criminal actors browse Web sites such as zillow.com and flipkey.com to identify and target realtors. Criminal actors also use Internet chat rooms to communicate with one another the details of the scheme, content of language used in spam and malicious links sent to victims.

- Financial institution reporting indicates Florida-based money mules[c] are establishing shell companies[d] using Florida's Department of State, Division of Corporations, online business incorporation portal at www.Sunbiz.org to give legitimacy to the EAC scheme and enable the opening of national bank accounts.

- As of January 2017, in a scheme targeting a Florida real estate transaction, a criminal actor compromised the e-mail account of the Michigan title agency assigned to the closing. Once the criminal actor determined the buyer's identity, the criminal actor used a spoofed e-mail account similar to the title agency's to instruct the buyer to wire funds from his local bank in Florida to a business account at a national bank located in New York controlled by a money mule. The money mule subsequently sent it on to his personal account at a local bank in Connecticut.

- As of January 2017, the president of a local Memphis real estate company stated his company has been victimized by EAC almost daily. After gaining access to the company's real estate agents' e-mail accounts, unknown subject(s) sent e-mails to homebuyers with instructions to wire payments to accounts controlled by subjects in Ghana. One subject received at least $2.2 million in fraudulent proceeds from individuals throughout the United States, with $400,000 attributed to fraud against multiple real estate agents, closing and title companies, and homebuyers in the Memphis area.

[c] Money mules are defined as persons who transfer money illegally on behalf of others.

[d] Shell companies are legal business entities registered or incorporated under the respective laws of one of the fifty states of the US, but which do not conduct actual or legitimate business activities, and which do not have significant financial or physical assets in the United States. Shell companies are simply paper corporations which do not have actual physical locations in the US, but, rather, may maintain mailing addresses or virtual storefronts (i.e., websites on the Internet) which give them the appearance of legitimacy.

- An identified network of money mules operating in Youngstown, OH, and Atlanta, GA, as of 22 January 2017 were perpetrating EAC by inserting themselves within the real estate settlement process, according to a multi-jurisdictional FBI investigation. The scheme, originating from Nigeria involves more than 260 compromised victim e-mail accounts, in excess of 350 accounts created and used by more than 20 money mules, and the use of more than 60 US and African-based bank accounts. This network reportedly is responsible for more than $6 million in verified victim losses.

Two recent real estate settlement fraud trends involve the exploitation of local and community banks originating and receiving fraudulent EAC real estate settlement-related wire transfers, and a notable increase in the reporting of real estate closing funds wire transferred to Mexican bank accounts.

- As of 31 March 2017, the FBI Internet Crime Complaint Center indicates consumers reported more than $2.7 million in illicit real estate settlement-related funds were sent to financial recipients in Mexico during the first three months of calendar year (CY) 2017, up from more than $400,000 reported during all of CY 2016.

The Office of Private Sector and the Criminal Investigative Division encourage partners in the financial services sector to conduct awareness and outreach campaigns to warn consumers about the dangers of e-mail account compromise techniques used to infiltrate and profit from real estate settlement transactions and to conduct additional due diligence on wire requests from customers conducting real estate transactions.

If you are aware of any persons or entities that were targeted by EAC schemes, please contact your local FBI field office.

Comments and queries regarding this LIR may be directed to the OPS Sector Analytic Unit at 202-436-8136, SAU@fbi.gov.