SafeAlert®

Loss Control Advisory Bulletin from ABA Insurance Services

Be vigilant against rapidly evolving fraud schemes

FBI notes actual fraud-related claims in Senate Judiciary Committee Testimony

June 9, 2020, the FBI's Calvin A. Shivers gave a statement before the Senate Judiciary Committee discussing the rapidly evolving fraud schemes exploiting the recent pandemic and how they were addressing these crimes. Most alarming is that *"the COVID-19 pandemic has only served to increase the number of stimulus, healthcare, bank, elder, and government fraud schemes.* ***As of May 28, 2020, the Internet Crime Complaint Center (IC3) received nearly the same amount of complaints in 2020 (about 320,000) as they had for the entirety of 2019 (about 400,000).*** *Approximately 75% of these complaints are frauds and swindles, presenting a challenge for the FBI's criminal program given the sheer volume of submissions."*

Of interest are the real situations involving financial institutions and their customers being targeted by scammers under the guise of the Paycheck Protection Program and swindled through Advance Fees and Business Email Compromise (BEC) schemes. Below are actual claims examples presented by the FBI:

- **A financial institution received an email, allegedly from the CEO of a company**, who had previously scheduled a transfer of $1 million, requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." **The email address used by the fraudsters was almost identical to the CEO's actual email address, with only one letter altered.**
- In another instance, **a fraudster spoofed the email address of a CEO who had been approved for a PPP loan, contacted the financial institution facilitating the loan and requested that the PPP funds be transferred to a new account at a different institution.**
- Multiple incidents have been reported in which state government agencies, attempting to procure ventilators or PPE, wire transferred funds to fraudulent brokers and sellers in advance of receiving the items. The brokers and sellers included both domestic and foreign entities. In one case, an individual claimed to represent an entity with which the purchasing agency had an existing business relationship. By the time the purchasing agencies became suspicious of the transactions, much of the funds had been transferred outside the reach of U.S. law enforcement and were unrecoverable.

Please share the following BEC protection tips from the FBI with your employees and your customers, and remind them to remain ever attentive and diligent in protecting their valuable assets:

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information.
- Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.

Continued ⇨

- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

The complete FBI Statement to the Senate Judiciary including information on other recent criminal activities such as Money Mules, Health Care Fraud, and Virtual Assets is available on the FBI's website at **https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic**.

For more on Business Email Compromise scams, visit **https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise**.

Additional loss control resources for your bank are available on **Insights at abais.com**.

ABA Insurance Services | MEMBER OF GREAT AMERICAN INSURANCE GROUP

Visit abais.com for more loss control information or to view this SafeAlert bulletin online. To subscribe to SafeAlert®, request reprints, or if you have questions about this bulletin, please contact ABA Insurance Services at marketing@abais.com or 800-274-5222.