5 fraud threats to watch in 2023

Future of Fraud Forecast examines common attacks on the rise.

February 16, 2023

Brock Fritz

Fake texts. Fake jobs. Fraudulent social media accounts. Technology has increased the ways in which fraudsters can attack businesses and consumers.

“As fraudsters become more sophisticated and opportunistic, businesses need to proactively integrate the latest technology, data, and advanced analytics to mitigate the growing fraud risk,” says Kathleen Peters, chief innovation officer at Experian Decision Analytics in North America.

Experian’s 2023 Future of Fraud Forecast expects fraud to surge this year amid uncertain economic conditions. To combat against fraud losses,

consumers and businesses can increase awareness by reviewing Experian's top five fraud predictions for 2023:

1. **Fake texts from the "boss."** Remote work has made it more difficult for some employees to communicate with their bosses. Therefore, Experian predicts a sharp rise in employer text fraud. The most common example of employer text fraud is when a fraudster impersonates an employee's boss in a text asking the employee to buy gift cards and forward the numbers and codes.

2. **Fake job postings and mule schemes.** The forecast predicts economic uncertainty will lead fraudsters to create fake remote job postings. The goal is to lure job applicants to provide their Social Security number, date of birth, and other private information that can be used to commit identity theft.

   Similarly, mule recruiting schemes occur when people accept remote jobs and unintentionally re-ship stolen goods or move fraudsters' money through their personal bank accounts.

3. **"Frankenstein" shoppers.** Synthetic identity fraud involves a fraudster combining real and false information to create a synthetic, or "Frankenstein," identity. The fraudster uses that identity to open lines of credit, eventually maxing out their credit limit with no intention of paying it back.

   Experian predicts a new version of synthetic identity fraud, in which fraudsters use synthetic identities and stolen payment cards to create online shopper profiles, could result in major losses for retailers.

4. **Social media commerce fraud.** In-app social commerce fraud could result in millions of dollars in losses. With easy access, little identity verification, and few fraud detection controls in place, social commerce makes retailers easy targets for fraudulent purchases.

5. **Peer-to-peer payment problems.** Fraudsters will use social engineering techniques to gain unauthorized access to peer-to-peer payments to get consumers to buy fake items or give up their account credentials. Once a consumer is lured into sending money, there are limited ways for them to recoup their losses because peer-to-peer payments move money instantaneously and irreversibly.

Looking back to last year's predictions, Experian's 2022 Future of Fraud Forecast identified these five threats:

1. **Buy now, pay later** lenders seeing an uptick in identity theft and synthetic identity fraud.
2. **Cryptocurrency scams** in which fraudsters set up accounts to extract, store, and funnel stolen funds.
3. **Ransomware attacks** in which fraudsters steal data and ask companies for large ransoms to gain back control.
4. **Online romance scams** in which fraudsters set up dating app profiles and ask people they meet for money or "loans."
5. **Digital elder abuse** stemming from fraudsters targeting digital newbies through social engineering and account takeover fraud.