Five fraud threats to watch for during economic recovery

In January, we shared our predictions for five fraud threats facing businesses in 2021 as a result of the COVID-19 pandemic, associated economic shift and the digital evolution. Now that we've reached the midway point of the year we've updated our predictions to reflect the current climate.

Putting a face to Frankenstein IDs: synthetic identity fraud

What it is: Synthetic ID (SID), also called Frankenstein ID, occurs when a fraudster fabricates an identity for the purpose of committing fraud. An augmentation of SID uses AI technology to create deepfake images. These images look like real people — talking, blinking and even changing facial expressions. Adding the deepfake aspect to SIDs can trick biometric sensors, because the SID is linked to what appears to be an actual person.

Prevalence: This is the fastest-growing type of financial crime with losses of $6 billion a year, according to Federal Reserve estimates. Other sources find 80 percent of credit card losses come from SID theft with an average loss of $6,000 per incidence.

Outlook: As methods for fraud detection mature, we expect fraudsters to rely on fake faces for biometric verification, using AI to combine facial characteristics from different people to form a new identity.

Overexposed: account application fraud

What it is: Fraudster uses stolen identities and Social Security numbers (SSNs) to create accounts using a customer's profile to steal as much as possible as quickly as possible.

Prevalence: This isn't new but it's becoming more sophisticated and done on a larger scale. In 2020, the rate of new account credit card fraud attempts rose 48 percent.

Outlook: Some estimate that up to 80 percent of SSNs have been exposed on the dark web, exposing a majority of Americans to this vulnerability; each successful credit card account fraud attempt can result in a $1,000 loss, on average, for a financial firm.

The heist: account takeover fraud (ATO)

What it is: Fraudster gains control of a customer's credentials, accesses their account and changes information, such as login credentials. A typical scenario includes the criminal taking over a deposit account and transferring money out of it. In a worst-case scenario, ATO can lead to emptying a customer's life savings.

Prevalence: In 2020, ATOs accounted for 54 percent of all fraud attacks, up from 34 percent in 2019. Growth can be partly attributed to increased capabilities of bots. More than 40 percent of online login attempts last year came from attackers trying to infiltrate accounts.

Outlook: Surges in data breaches, advances in automation, expanded online banking services and vulnerabilities exposed from social engineering mistakes are leading to rises in account takeover fraud. Prior to the pandemic, average losses increased 69 percent year-over-year and were approaching $2,000 per ATO case, for a total loss estimated at $6.8 million annually.

Overstimulated: relief fraud activity

What it is: Three rounds of government-issued stimulus funds since the start of the pandemic were a welcome relief for many, but also an easy target for fraudsters. The vast number of unemployment claims create another vulnerability for payment scams.

Prevalence: As a result of interstate criminal organizations, states are experiencing unemployment fraud at a much greater rate than previously understood. For example, in January 2021, the state of California reported $11.4 billion had been confirmed as fraudulent unemployment claims, with nearly all fraudulent claims made through the federally supported Pandemic Unemployment Assistance program.

Outlook: We predict fraudsters could take advantage of ongoing relief payments by using stolen data from consumers, including unemployment relief and advance child tax credit payments that begin in July 2021 and continue monthly through the rest of the year.

Behind the times: digital readiness lag

What it is: The sudden onset of COVID-19 forced businesses to quickly pivot to digital platforms, and some were more prepared than others. Businesses should expect to invest, not only to catch up, but to stay current in technologies and infrastructure that protect their customers and bottom lines from cyberattacks, data breaches and other vulnerabilities.

Prevalence: In a recent survey, when asked to what extent the budget for consumer lending technology was expected to change, 29 percent of businesses stated they planned for a substantial increase, indicating that digital readiness in fraud prevention is important enough to be a top priority.

Outlook: Fraudsters seek the paths of least resistance. We predict businesses with lackluster fraud prevention tools and insufficient online security technology will experience more attacks and suffer larger-than-average financial fraud losses in 2021 and beyond.

Looking ahead

As the immediate threat of the pandemic wanes and we continue to reopen the country, new opportunities arise for consumers, businesses and fraudsters. Businesses are changing to meet consumer expectations, but they must balance the desire for seamless experiences with the need to mitigate fraud. Understanding existing and future fraud threats can help businesses succeed in the long term.

Learn More: **experian.com/fraud-resource-center**

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 855 339 3990
www.experian.com