Upcoming fraud trends and how to combat them
Trends, technology and tactics that help and hinder

Both businesses and consumers have greater confidence in biometrics, but they’re not yet ready to say goodbye to passwords. Going forward, firms that aspire to be leaders in customer experience will have to marry the two, which means embracing the concept of leveraging identity data and biometric technology.

Fraud is hitting new types of customer accounts. Businesses have limited experience fighting fraud in these areas. Since consumers typically don’t keep a close eye on these accounts, this may end up being a perfect (fraud) storm.

Fraudsters are sophisticated, and they’re always looking for new ways to take over identities and invade your portfolio. We can help you determine the best strategy, data and tools to protect your customers and your bottom line.

Mobile account takeovers rates have increased by 2x each year for the past four years.

In 2018, there were 679,000 mobile account takeover victims — that’s the size of El Paso, Texas.

Mobile channels have increased consumer convenience. Unfortunately, they’ve also increased fraud risk.

Targeting loans has been a lucrative move for fraudsters — especially because businesses and consumers aren’t likely to become aware of these attacks.

A lot of financial and reputational damage can occur in two months. Protecting customers and your business isn’t a one-and-done activity. Now is not the time to let your guard down.

66% of consumers still have confidence in visible signs of security to feel safe (PIN codes, passwords, security questions).

74% of consumers indicated greater confidence in a business that uses biometrics.

Fraud rates have increased by 103% among loyalty and rewards points over the past year.

Fraud rates have increased by 180% among retirement accounts, such as IRAs or 401(k) plans, over the past year.

Fraud rates have increased more than 2x for car loans, mortgages, student loans and HELOCs over the past year.

Targeting loans has been a lucrative move for fraudsters — especially because businesses and consumers aren’t likely to become aware of these attacks.

Fraudsters successfully create and misuse new accounts for an average of 54.2 days before being detected.

A list of financial and reputational damage can occur in two months. Protecting customers and your business isn’t a one-and-done activity. Now is not the time to let your guard down.

Fraudsters are sophisticated, and they’re always looking for new ways to take over identities and invade your portfolio. We can help you determine the best strategy, data and tools to protect your customers and your bottom line.

Learn more from the e-book

Learn more