epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER
The inside scoop on payments for businesses of all sizes

Top 10 Fraud Trends in 2023

The following article originally appeared on Fraud.com.

Fraudsters will always seek new ways to exploit people's private information.

Cybercrime and fraud prevention is an ever-changing and evolving field based on varied tactics used by fraudsters. While fraudsters will always seek to conduct new fraud forms, you can be better prepared to mitigate their risks.

One place to start is being aware of the most frequent fraud attacks today. Here are the top 10 biggest fraud trends you need to know for 2023.

1. Automation

Automation makes it easier for criminals to exploit users' accounts while remaining undetected themselves, increasing the risk of fraud. With automation, fraudsters use software or bots to accomplish tasks that otherwise require human intervention, thus covering more ground. For example, credential stuffing is the act of testing stolen or leaked credentials on websites and services at scale to see if they work on any accounts.

2. Account Takeover

Account takeover (ATO) is a type of identity (ID) theft that occurs when a fraudster gains access to an individual's or company's computer accounts, email accounts and other personal information. In a typical ATO attack, hackers use phishing and malware methods to acquire legitimate user credentials or buy them from the dark web; they then use stolen credentials for account takeover.

Automated takeover attacks are carried out using stolen credentials, and organizations are particularly vulnerable to these attacks. A takeover can lead to a variety of crimes and direct financial losses, including:

- Bank account takeovers (current accounts, credit cards)
- Money laundering
- Stealing loyalty or rewards points
- Reselling subscription information

3. Adoption of New Digital Payments and Methods

Digital payment platforms and cryptocurrencies disrupt traditional payments, allowing consumers and businesses to make payments more quickly and efficiently. Technologies that enable new ways to pay are also open to new avenues of attack from fraudsters, as they use stolen credentials to carry out fraud and ID theft. Cryptocurrencies, while not quite mainstream in their use yet, are growing in popularity, and the anonymity provided by these currencies makes it easy for criminals to carry out illicit activities.

4. Ongoing Challenge of Balancing Fraud & Client Friction

Online businesses must balance risk and opportunity when mitigating fraud. In the case of online shopping, the amount of "friction" clients experience during the checkout process correlates with their conversion success.

The balance between friction and fraud becomes even more challenging across multiple channels, such as web, mobile and point of sale. Merchants and issuers seek alternative authentication solutions (such as passive behavioral biometrics and password-less authentication via biometrics with liveness detection) to attain this balance to improve customer experience and reduce risk.

5. Rise of Synthetic Identities

According to the McKinsey Institute, synthetic ID fraud is the fastest-growing type of financial crime in the United States and is also on the rise around the globe. Indeed, synthetic ID fraud comprises 85% of all fraud right now.

With this type of fraud, fraudsters create new identities by piecing together elements of a person's personal information and combining them with false identifiers. Essentially, they take bits of legitimate data, add fictitious information and create a new identity. Organizations are struggling to prevent synthetic ID fraud; after all, the whole point of synthetic ID fraud is to create a synthetic victim that does not exist in real life.

6. Escalating Cost of Fraud

The total cost of fraud is becoming a genuine concern, from fraud losses, prevention tools and headcount costs to the client lifetime value impact. It's estimated that fraud loss is $5.4 trillion globally; according to the University of Portsmouth, fraud accounts for approximately $185 billion in losses in the U.K. and a 9.9% increase in the cost of fraud for U.S. financial services firms.

Why the increase? As more and more people have turned to online and mobile channels to shop, fraudsters again have followed, thus the increase in fraud losses and associated costs with fighting fraud.

7. Growing Need for Multi-Layered Fraud Assessment

The digitization of e-commerce and banking is a well-established trend that shows no sign of abating; in parallel, fraud across these digital channels has remained a constant and relentless issue.

On the other hand, fraud prevention leaders are generally trying to defeat fraudsters with limited and siloed fraud management capabilities.

To achieve the best fraud prevention results, fraud prevention leaders must orchestrate all relevant data points, risk signals and client data to form a centralized and balanced response that reduces risk, client friction and associated prevention costs.

8. Targeted Attacks

Another growing threat is targeted attacks, which occur when cybercriminals compromise a target entity's entire infrastructure, including its network and computer systems. They can conduct such attacks anonymously and over a long period, gaining access to critical financial data and causing significant losses for institutions and constituents.

Targeted attacks occur in phases, thus are less likely of being discovered.

Although targeted attacks typically happen at the entity level and don't target specific consumers, these attacks put client information at risk and can harm an organization's reputation.

9. Heightened Need for Real-Time Risk Assessment

As online and mobile app usage increases, there's a growing need for comprehensive fraud detection, identity verification and authentication solutions to unite. Such solutions call for real-time risk assessment that leverages the latest AI, machine learning and fraud orchestration tools to manage the client's risk collectively and trust, utilizing all associated risk signals to drive fair and balanced client satisfaction.

10. Account Security

To protect against fraudsters, organizations need to take a layered approach to account security. The culprit behind system attacks is often single-factor authentication methods that result in unauthorized access to accounts, enabling client account fraud, identity theft, ransomware attacks and other fraudulent activity, notes the Federal Financial Institutions Examination Council.

With multi-factor authentication, institutions use more than one distinct authentication factor to successfully authenticate clients, such as behavioral biometrics, device ID and biometric authentication.

Get Ahead of Fraud Trends

Throughout the client journey, it's essential to incorporate safety measures that protect organizations and their users, prevent disruptions in the buying process and keep fraudsters at bay. If you have any questions, reach out to your financial institution.

Source: Fraud.com

epcor®

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha®
Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665