CROSSFIRST BANK®

Treasury Notes

SUMMER & FALL 2023

Inside this Issue

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.

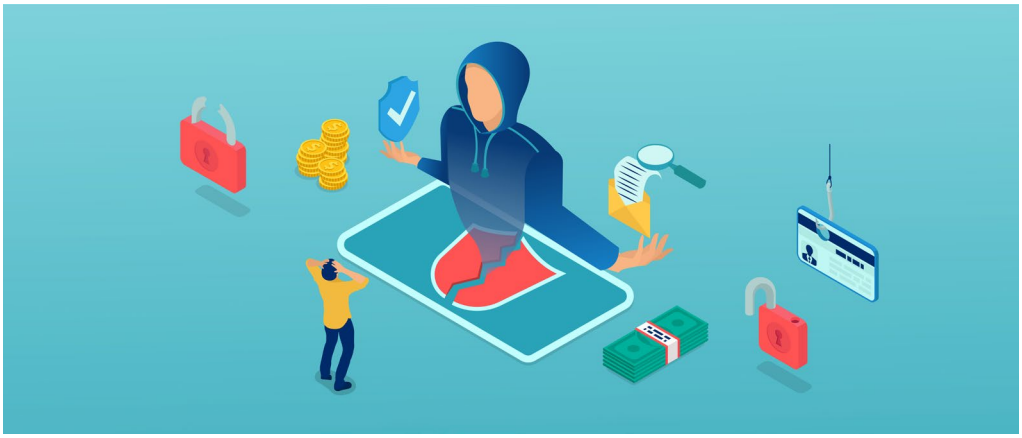
One place to start is being aware of the most frequent fraud attacks today. Here are the top 10 biggest fraud trends you need to know for 2023.

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



see FRAUD TRENDS on page 2

Don't Fall Victim to Current Debit Card Fraud Trends

by Trevor Witchey, AAP, NCP, Senior Director, Payments Education, EPCOR

EPCOR's team has continuously heard tales about debit card theft and fraud. While creating duplicate cards is harder than ever, thanks to most cards having an EMV chip and many merchants installing EMV chip reading devices, debit card fraud is still an ongoing issue due to cards being stolen, devices being hacked or stolen and databases containing debit card information being breached.

Current fraud trends to watch:

- **Fraud at Retail Stores.** Financial institutions are seeing an increase in debit card theft happening at retail stores. For example, wallets are being stolen from purses while the cardholder is waiting in line at the checkout or while chatting with the cashier. Then, the thief takes the stolen debit card to another retailer to buy goods and makes the purchases on EMV-ready devices. A

see DEBIT CARD FRAUD on page 3

FRAUD TRENDS continued from page 1

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.

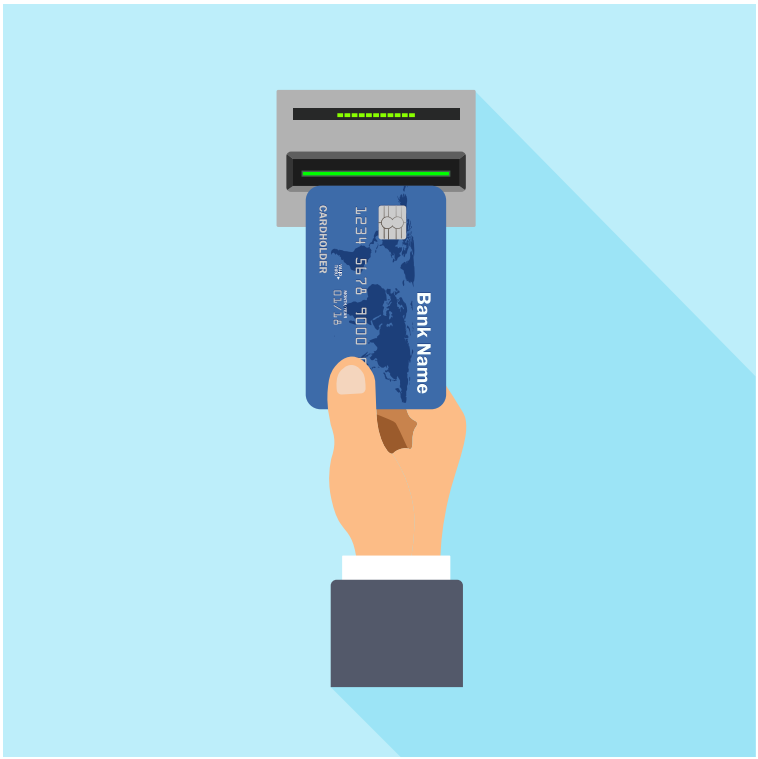
To achieve the best fraud prevention results, fraud prevention leaders must orchestrate all relevant data points, risk

see FRAUD TRENDS on page 6

DEBIT CARD FRAUD continued from page 1

big issue here is you cannot charge the funds back to the merchant via the card network because they have EMV devices installed. This creates pain in the form of Reg E write-off losses when handling disputes because the stolen Debit Card led to unauthorized charges.

- **Social Scamming.** There are many scams where fraudsters reach out via phone calls, emails, social media and other available avenues to request an account holder's debit card number. Many account holders are receiving scam emails or phone calls from fraudsters posing as their own financial institutions. Please note:
  - ⇨ A person's debit card is theirs and theirs alone. The information should not be shared with anyone. Everyone should guard this information like you would your social security number.
  - ⇨ A financial institution will never directly request information such as a person's debit card numbers, as they already have that kind of account information on file.
  - ⇨ Account holders should never give out their login credentials to anyone for online banking systems or apps for any reason.
- **Fraud Using Digital Wallets**. This type of fraud appears to be on the rise, as fraudsters are stealing card info and then inserting said information into their own digital wallet, such as Apple Pay, Google Pay, Samsung Pay or their own financial institution. Then, they'll just tap their phone at a retailer that accepts Near Field Communication (NFC) based payments or use whatever apps accept digital wallet payments. As an FYI, when the phone is tapped at an NFC device, that is a "point of sale card present" payment whereas goods/services purchased from an app is considered "card not present".
- **ATM Skimmers.** There are still ATM skimmers out there, whether that is placing a device over the card reader or drilling holes in the ATM to insert a skimmer on the chipset. However, lately, fraudsters are getting even more clever and are creating devices small enough to be inserted into the card reader itself to steal information. Additionally, phony panels that look exactly like what is normally on an ATM are being inserted, and they have tiny pinhole cameras to watch for PIN entry. While skimming technology may be difficult to overcome, advising your clients to cover their hand while entering their PIN could help reduce the incidence of fraud on their card.



Here are a few additional debit card fraud prevention tips:

- Safeguard your debit card, smartphone and computers.
  - ⇨ Keep your cards and devices in safe locations and out of reach.
  - ⇨ Implement complex passwords/passcodes, both to unlock the device and to access accounts on Apps and websites.
- Anytime you can use Out-of-Band Authentication (OOBA) to verify any payments performed on apps or websites, the better.
- Always be careful where you swipe your card.
- Utilize online banking either in website form or your financial institution's app to check your online statement daily for any out-of-the-ordinary transactions. Make it a habit to check your account activity at least once daily and opt-in to receive alerts for account transactions.
- Look out for each other. If you see any friends, family, co-workers or even complete strangers appearing to fall victim to a scam, speak-up and say something if you feel comfortable doing so. Sharing information can help reduce the incidence of fraud.

Stay safe out there! And if you're looking for additional information on how you can avoid fraud, visit epcor.org/corporateuser for more corporate-focused fraud education and EPCOR's YouTube channel for short informational videos.

Fast, Faster or Instant: What's Your Payment Preference?

by Shelly Sipple, AAP, APRP, NCP, Senior Director, Certifications & Continuing Education, EPCOR

When it comes to making a payment, a payment is a payment is a payment, right? Yes, in the sense that a consumer or business intends to pay for goods or services. And while your financial institution likely offers a variety of options, how might your organization choose one payment means over another?

Perhaps one consideration is whether your organization wants to fund the purchase out of current income or with borrowed funds. Some other reasons may include ease of use, familiarity, convenience and cost. Or your organization may prefer to use a payment method that is safe and secure or universally accepted. However, in today's ever-changing (and rapidly) payments ecosystem, consumers and businesses may also make the decision based on how quickly the payment needs to be in the payee's account—fast, faster or instantly.

But what payment options are considered fast? Faster? Instant? Cash would be considered fast when compared to bartering as are checks, debit cards and next-day ACH. However, Same Day ACH and wire transfers fall into the faster category. And that leaves RTP® and FedNow℠, which are instant payments. While fast payment options are good and still serve a purpose, faster and instant payments are what many organizations are interested in these days. So, let's further define them!

Faster Payments

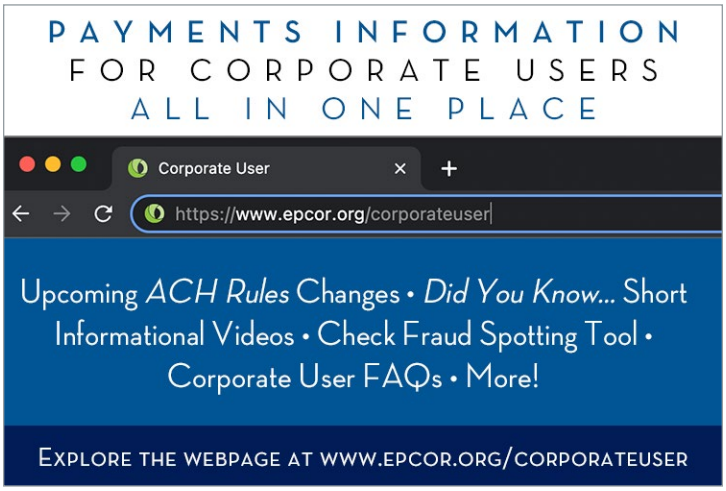
With faster payments, a payee's deposit account is credited or debited a few hours after a payment order has been initiated. Same Day ACH allows credit and debit payments to be originated, processed and settled all on the same day. Same Day ACH payments are accumulated throughout the day and then offset against each other, with only the net differential transferred between financial institutions (known as deferred net settlement). A wire transfer is also a faster payment; however, individual transactions settle as they are processed (known as real-time gross settlement). Both Same Day ACH and wires may only be processed during certain hours Monday through Friday, excluding federal holidays. This is one key feature that keeps them from being instant payments.

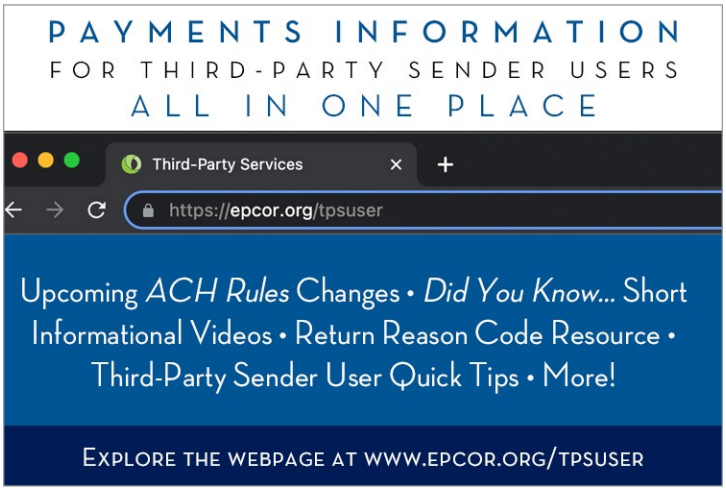
Instant Payments

With instant payments, clearing and settlement occur in real-time for each individual credit transaction, and funds can be sent and received around the clock, any day of the year. The transfer of funds between the payer and payee's accounts at financial institutions occurs within seconds and funds are final and irrevocable. RTP®, which was implemented November 2017, and FedNow℠, which goes live July 2023, are examples of instant payments.

RTP® and FedNow℠ are different from ACH in the fact that the systems operate on a 24/7/365 basis. Gone are the constraints of normal banking hours. Along with a completely wide-open timeframe, RTP® currently can be, and FedNow℠ will be, utilized by consumers, businesses and financial institutions. Anyone anywhere can participate in instant payments (as long as they have connection to the given network). These benefits of speed, convenience and accessibility are what set RTP® and FedNow℠ apart from traditional payment methods.

Interested in utilizing some form of faster or instant payments at your organization? Reach out to your financial institution to learn more and discuss your options.

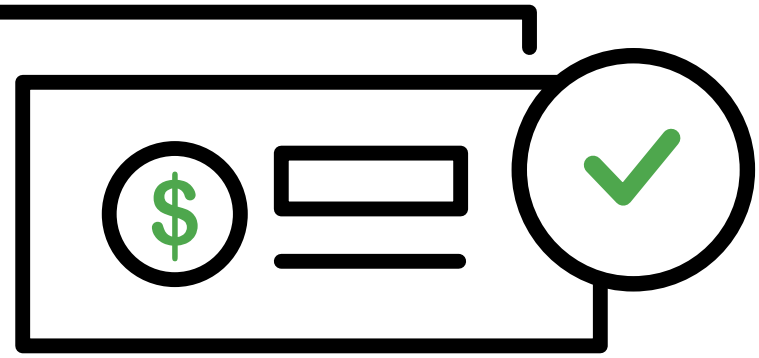




The Check's in the Mail... Or Is It?

by Marcy Cauthon, AAP, APRP, NCP, Senior Director, On-Demand Education, EPCOR

How many of us have ever put an outgoing bill/invoice in our home/business mailbox or a blue U.S. Postal mailbox? It is true that Americans have decreased their use of check payments, however; cases of check fraud continue to soar. Criminals are targeting USPS blue collection boxes, unsecured residential mailboxes, privately owned cluster box units at apartment complexes and high-density commercial buildings to gain access to funds to perpetrate a scam.



After stealing checks from a mailbox, fraudsters will alter or "wash" the check, replacing the Payee name with a fraudulent consumer or business name and deposit the checks into fraudulent accounts they have set up. They often will wash and alter the amount of the check as well. Fraudsters have also gotten crafty at stealing business checks and creating authentic-looking counterfeit checks that are utilizing real account and routing numbers but are deposited using fake identities.

Why has this type of fraud become so profitable for fraudsters? Well, there are numerous ways checks may be deposited in today's environment that give immediate availability but have less monitoring, such as image-enabled ATMs and remote deposit capture.

What can consumers and businesses do to combat this type of fraud? Be vigilant in reviewing your transactions online with your financial institution daily if not more often.

Why is remaining vigilant so important? Financial institutions only have a 24-hour window to return a check after it has been posted to your account. That is a very quick turnaround. Outside of that timeframe, your financial institution may be able to deal directly with the depositing financial institution to try and recover funds for altered checks or forged endorsements. With the number of these claims flowing through the financial system today, it could take months up to a year to get the issue resolved, but it is not guaranteed that funds will be reimbursed.

Reviewing your transactions daily is imperative, especially if you are a business that has had your checks counterfeited. Again, your financial institution only has 24 hours from when the item posts to your account to get it returned. Your financial institution will have a timeframe specified within their deposit agreement of how long they give you to review your account statement and report that an item is altered or counterfeit. It is important that your business is aware of that timeframe, as the loss could fall on you if you don't notify your financial institution in a timely manner.

Another major issue that could impact your organization is when a check payment sent to you by your client is intercepted by a fraudster. This scam causes issues for the business and the consumer. The consumer believes they paid their bill/invoice on time, and the business is sending out late notices as they never received the payment. My advice to your business in this situation is to work with your consumer to resolve the error. The consumer will need to contact their financial institution and notify them that the check cleared their account but that the named Payee (your business) didn't receive the funds as intended. The financial institution will then need to file a claim to the depositing financial institution on the consumer's behalf, which often requires a written statement from your business stating you never received the funds.

The Financial Crimes Enforcement Network (FinCEN) issued an alert earlier this year to financial institutions with tips on how to detect, prevent and report suspicious activity associated with mail theft-related check fraud. Some of the red flags that financial institutions are looking for are:

1. Non-characteristic large check with-drawals on accounts with a new Payee.
2. Account holder claims a check they put in the mail was never received by the recipient, however; the check cleared their account.
3. Checks clearing on accounts appear to be a different color or not within the check range of other checks issued.
4. Account holders with no history of check deposits start experiencing large check deposits followed by a rapid withdrawal or transfer of funds.
5. Checks have appeared to have been washed using chemicals and Payee and/or amounts have been altered.

Combatting this type of fraud begins with account holders being diligent in reviewing their account history via their institution's online banking or utilizing a positive pay service that your institution may be offering to your business. If you have any questions about your responsibilities as an organization, contact your financial institution.

Sources: ABA, Sterling Compliance

FRAUD TRENDS continued from page 2

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