Early Warning®

Spot & stop payments fraud:

An in-depth look at payments fraud prevention

WHITE PAPER

Introduction

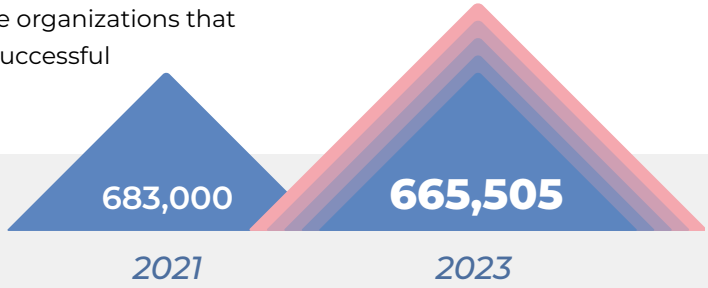
Payments fraud is nothing new, but the sheer volume and escalation of losses for financial institutions (FIs) year over year is.

Faster payments options like same-day ACH are quick and convenient for consumers, but criminals are taking full advantage of these new and exciting technologies too. In fact, instances of fraud via faster payment methods have risen since 2021.

ACH fraud losses have increased 47 percent between 2021 and 2023 and the trend continues[1]. It is a top concern, with 33 percent of organizations reporting they experienced ACH debit fraud activity and 19 percent of organizations reporting ACH credits fraud activity. Of the organizations that were victims of payments fraud attacks, only 41% were successful in recouping most of the funds.[2]

Long-standing payment methods like checks were no exception either.

Check fraud remains an ongoing threat, with 65% of organizations reporting fraud attempts from checks according the 2024 AFP® Payments Fraud and Control Survey Report.[3]



*Suspicious Activity Reports (SAR) Stats revealed that banks filed **680,000 check-fraud reports in 2022** compared to just 350,000 the previous year.*[4]

CLICK HERE TO LEARN MORE

Underinvestment in payments fraud prevention can quickly turn into a nightmare, and trying to play catch-up is a highly risky and expensive strategy. With schemes like fake merchant fraud, ACH fraud, account takeover, and check fraud more rampant than ever, how can FIs get ahead of payments fraud and stop it at the source?

Using advanced technologies powered by predictive analytics and machine learning, FIs are successfully preventing a myriad of payments fraud attempts.

*In this report, we'll look at **the current payments fraud landscape, the core challenges FIs face in the prevention of it, and how predictive intelligence and consortium data play a key role** in mitigating the problem, reducing losses, and improving the customer experience.*

CLICK HERE TO LEARN MORE

Today's payments fraud landscape

Payments fraud comes in a variety of forms and is continually evolving as new technologies emerge. Generally, payments fraud encompasses any type of unauthorized transaction that uses false or stolen payment information including ACH transfers, counterfeit or altered check payments, account takeovers, and/or the use of fraudulent bank accounts opened using stolen or manipulated identities.

More recently, criminals have also pivoted to new strategies like manipulating consumers into authorizing fraudulent payments for them using techniques such as romance scams and social engineering.

Fraud vs. Scam

What's the difference?

A basic way to differentiate fraud and scams is *unauthorized* vs. *authorized* transactions:

Fraud

Someone gains **unauthorized access** to a bank account and makes a payment/steals money without the account owner's permission or involvement in the transaction.

Scam

An account owner is knowingly involved in a transaction and authorizes a payment to be sent. Even if an account owner is tricked or persuaded into **authorizing a payment** for a good or service they never receive, this is considered a scam.

CLICK HERE TO LEARN MORE

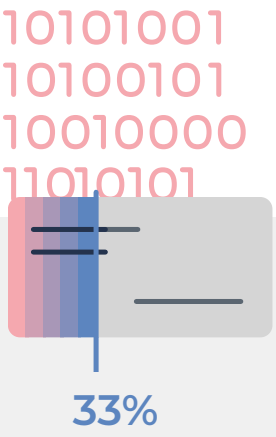
These scams and fraud attacks can equate to big losses for FIs, especially when it comes to credit card payment losses. Bad actors often use these payments fraud methods to fraudulently pay off credit card bills, helping them build credibility over time and access higher and higher lines of credit until they eventually "bust out," maxing out their credit without any intention of repaying the bank.

ACH fraud

The Automated Clearing House (ACH) Network is used to facilitate electronic payments and money transfers between bank accounts. It's commonly used by businesses to send direct deposit payments to employees and pay vendors, but it's also used by individuals to send peer-to-peer (P2P) payments, make credit card or bill payments, and send tax payments to the government.

ACH transfers offer low processing costs and are easy to use, making them a popular and ubiquitous payment option for businesses and consumers alike. For these reasons, the ACH Network processes a very high volume of transactions, with over $80.1 trillion in payment value processed in 2023 alone.[5]

While ACH transfers are convenient for legitimate users, bad actors have also found ways to exploit the payment network for their own nefarious purposes. In 2023, ACH debit fraud accounted for 33% of payments fraud, up from 30% in 2022, and ranked as the second most popular payment method targeted by fraudsters, second only to checks.[6]



*In 2023, **ACH fraud accounted for 33%** of payments fraud.*

Criminals commit ACH payments fraud in several ways. Fraudsters can gain access to a compromised or fraudulent account and initiate an ACH debit to do things like pay off a loan, initiate a monthly bill pay, or even send a payment to an account of their own at another bank. They may also use imposter scams to trick individuals into making ACH transactions that send money to an account the scammer controls.

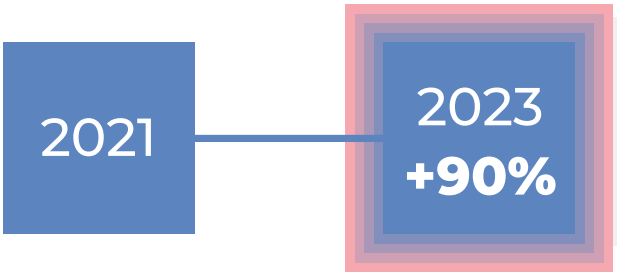
Ultimately, FIs are liable for losses incurred by consumers due to fraudulent ACH transactions, meaning they can be responsible for big losses if the problem is left unmitigated.

CLICK HERE TO LEARN MORE

Check fraud & fraud via business checks

Convenient payments options like debit and credit cards, same-day ACH, and P2P payments apps have become the most widely used payment methods in recent years, but checks are still commonplace—and criminals have been exploiting them for fraud at an alarming rate.

Check fraud has recently escalated drastically, increasing 96% in 2022 over the previous year and has remained at an elevated level in 2023. And while the total volume of checks written has gone down, the average check value has shot up from $673 in 1990—or $1,602 in today's dollars—to $2,684 in 2023.[7]



*Check fraud has recently escalated drastically, **increasing 90% in 2023** over the previous two years.*

The dramatic increase in check fraud has been attributed in part to criminals targeting the U.S. mail system to steal checks, which they then alter or use to create counterfeits. The problem has become so bad that postal authorities and banks have warned customers to avoid sending checks through the mail altogether.

Businesses have also become prime targets for check fraud attacks, with criminals taking full advantage of the fact that business checks are typically written for higher dollar amounts. In fact, a recent report from AFP cites checks as the payment method most vulnerable to fraud, with 65% of organizations reporting they faced fraud activity via checks in 2023.[8]

CLICK HERE TO LEARN MORE

Account takeover (ATO)

Account takeover occurs when an individual's bank account information is commandeered by a fraudster to steal funds or information.

Cybercriminals use techniques including social engineering, phishing, and skimming to steal consumers' payment information or trick them into handing it over. This type of fraud can be especially hard to detect because the transactions made appear to be coming from a legitimate customer in good standing with the FI.

While ATO has been an issue for years, the problem is on the rise, with losses of $13 billion in 2023, a 15% increase from the previous year.[9] 75% of North American FIs also report that they are concerned about a variety of fraud resulting from ATO, including third party ACH fraud, third-party person-to-person, wire fraud and third-party card fraud according to a recent survey by Datos Insights.[10]

Fake merchant fraud

Fraudsters are finding any gap where banks and credit unions have underinvested in past years, and FIs report they're seeing a sharp increase in fake merchant scams.

Merchant scams involve bad actors posing as legitimate businesses on ecommerce sites and other apps. These fake merchants may use the account to process payments using stolen cards or to trick customers into purchasing products that either don't exist or will never be delivered to them.

The most common type of merchant scam is a "bust out" scam, where the fraudster opens a merchant account and begins processing transactions and opening lines of credit. Once they've established a high credit limit or amassed a good amount of money from "selling" non-existent or counterfeit goods, they "bust out", maxing out their line of credit without repaying or cashing out the accrued funds and vanishing.

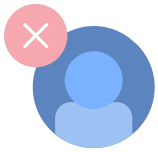
Merchant fraud is somewhat easy to identify once it's already occurred, but the problem is recouping the lost funds after the criminal disappears with the proceeds. Consumers may initiate a charge-back to be made whole again by their credit card provider, but this leaves FIs on the hook for taking the financial loss from this fraud scheme.

Challenges FIs face in detecting and preventing payments fraud

Liability for payments scams is shifting from consumers to FIs

Liability for fraud and scams has historically fallen somewhere between the consumer and their FI, depending on the type of fraud or scam committed. For example, individuals are currently responsible for losses incurred due to authorized payments scams, where a criminal convinces or tricks an individual into sending a payment using manipulation tactics like puppy scams, romance scams, or imposter scams. However, liability for scam losses is now heavily shifting to banks and credit unions, driving up operational costs and increasing financial losses for FIs.

FIs are also liable for losses from unauthorized ACH transfers, "bust out" fraud from criminals using synthetic identities, and losses from counterfeit or altered checks or duplicate deposits.



Impact on the customer experience

Payments fraud and the prevention of it can also heavily impact the customer experience. Today's customers expect fast, safe, and easy transactions facilitated by online banking—but faster payments expose consumers and FIs to more risk. While consumers enjoy the immediacy of faster payments methods like same-day ACH, exposure to fraud or scams can create a very negative customer experience and lead to loss of trust between the consumer and their FI.

FIs are faced with a balancing act. Removing friction from the payments process is paramount, but criminals exploit the float times between a transaction and when the accounts actually settle between banks.

Legal & non-compliance issues

Establishing a strong relationship with your FI's internal legal, risk, and compliance partners is challenging but critical to chipping away at the issue of payments fraud. Non-compliance with KYC and AML laws can mean hefty fines, reputational damage, and loss of customers.

Identifying and quantifying the different forms of fraud can be quite difficult. For example, it's often challenging for banks to differentiate between synthetic identity fraud, traditional identity theft, and first-party fraud. And without the ability to quantify the problem, it's hard to prove that fraud is happening.

However, banks and credit unions remain liable for ensuring their customers are who they claim to be and need to have robust tools in place to ensure they're compliant with KYC and AML laws.

CLICK HERE TO LEARN MORE

Predictive intelligence and the National Shared Database℠ resource

Predictive intelligence uses historical data to identify patterns and anomalies that help predict future behavior.

The **National Shared Database**℠ is a consortium of shared data contributed by over 2,500 FIs. The data is aggregated and analyzed to give FIs deep insights into things such as the likelihood that a new customer is using a synthetic or stolen identity, the likelihood that they'll commit first-party fraud, or the potential for them to incur non-sufficient funds returns.

Banks and credit unions often struggle to evaluate the risk of taking on a new customer when they only have internal data to work with. However, when banks can share information across institutions, suddenly they have much deeper insights into the risk profile of a given customer. In the case of payments fraud, our predictive intelligence solution uses account activity data from both participant and non-participant FIs, to create models that return predictive scores indicating the likelihood that a payment will return unpaid.

In 2023, ***Early Warning® alerted FIs $32 billion in high-risk transactions*** through the National Shared Database.

The **National Shared Database**℠ is an incredibly powerful tool in identifying and preventing fraudulent behavior.

The role of predictive intelligence in preventing fraud for credit card repayments

Payment Chek® Service from Early Warning, a predictive intelligence tool for payments fraud prevention, gives banks and credit unions deep insights that help them prevent fraudulent ACH transactions, identify counterfeit checks and duplicate deposits, and mitigate losses from P2P payments scams. This ultimately minimizes returns so that institutions can get paid on time.

Payment Chek® Service helps FIs answer the following questions before accepting a potential payment:

- Does the inquiry account data match with the account owner or account signer?
- Is the payment account open, closed, or overdrawn?
- What is the likelihood that this item will be returned unpaid?
- Is this payment being made with a duplicate or counterfeit item?

CLICK HERE TO LEARN MORE

Predictive intelligence powered by bank-contributed data models: Participant Model & Non-Participant Model

The models behind **Payment Chek**® are trained with data contributed to the **National Shared Database**℠ and can predict certain outputs given the inputs from this continuously updated data.

Using account activity data from both participant FIs (account status history and a rolling 180 days of check and ACH transactions) and non-participant FIs, the models behind **Payment Chek**® return predictive scores, indicating the likelihood that a payment will return unpaid, allowing inquirers to assess payment risk with precision.

- **Participant Model:** Provides unparalleled visibility into the return risk associated with ACH and paper check transactions, as well as the historical status for transactions drawn on an FI participant account.
- **Non-Participant Model**: Expands risk score coverage to transactions drawn upon FIs that do not directly contribute to the **National Shared Database**℠. Powered by machine learning, this model increases return risk responses to confidently cover more than 90% of all inquiries.

Benefits include:

- Enabling funds availability decisions when someone deposits or pays with an item drawn from an FI that directly contributes account status data to Early Warning
- Predicting the likelihood that an item (check or ACH) will be returned within 30 days
- Scores from 701-799 with a higher score indicating a higher likelihood the item will be returned

How it works in real time

Step 1

A customer presents a payment in person (check) or online (ACH).

Step 2

The receiving FI submits an inquiry to the Early Warning **National Shared Database**℠ Resource in real time to determine its risk score

Step 3

Early Warning responds with insight on: Account Status, Type of Account, Account Owner, Potential Risk of accepting

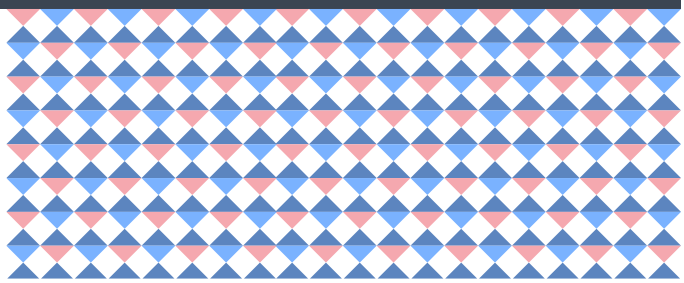
Step 4

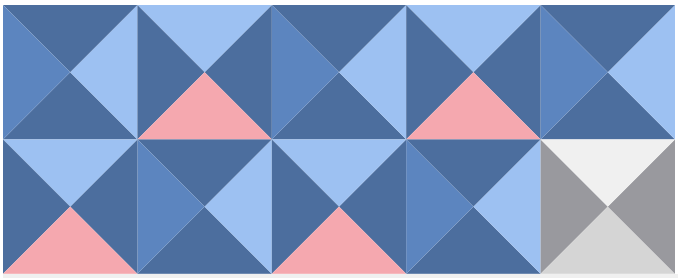
The receiving FI makes an informed decision on the payment based on the Early Warning response and its own risk tolerance

By mitigating the impact of payments fraud attempts, banks can prevent major losses for their credit card products.

CLICK HERE TO LEARN MORE

*In 2023, **Payment Chek®** helped the U.S. Financial System **prevent $126M in improper and fraudulent credit payments and identify 11 million payment transactions going to unauthorized accounts.***





***Nine out of 10 of the nation's largest banks in terms of DDAs use** Payment Chek® due to the high-quality data and extensive coverage the product provides in helping to prevent payments fraud.*

Key benefits of Payment Chek® for financial institutions

Account Owner Authentication (AOA) in real-time

The first step to preventing payments fraud is to verify that the person transacting on an account is the owner and thus authorized to make the transaction.

This is especially important when it comes to validating external accounts used for credit card payments, outbound wires, and disbursements. Confirming ownership and the standing of deposit accounts when the account is presented for a collection payment drastically reduces potential fraud losses.

The real-time nature of AOA means that you can protect your institution from losses while still maintaining a seamless experience for the customer—a win-win for both parties.

CLICK HERE TO LEARN MORE

Accelerate payment posting times and determine "open to buy"

Payment Chek® enables FIs to accelerate credit card payment posting times for low-risk customers, meaning the FI can determine the "open to buy" on an account quickly following a customer's payment. This allows the FI to release the full line of credit back to the customer within a short timeframe without taking on excessive risk.

Conversely, FIs can also identify high-risk payments in real-time by determining the likelihood that a payment will return unpaid, or that the item is a duplicate, counterfeit or otherwise altered.

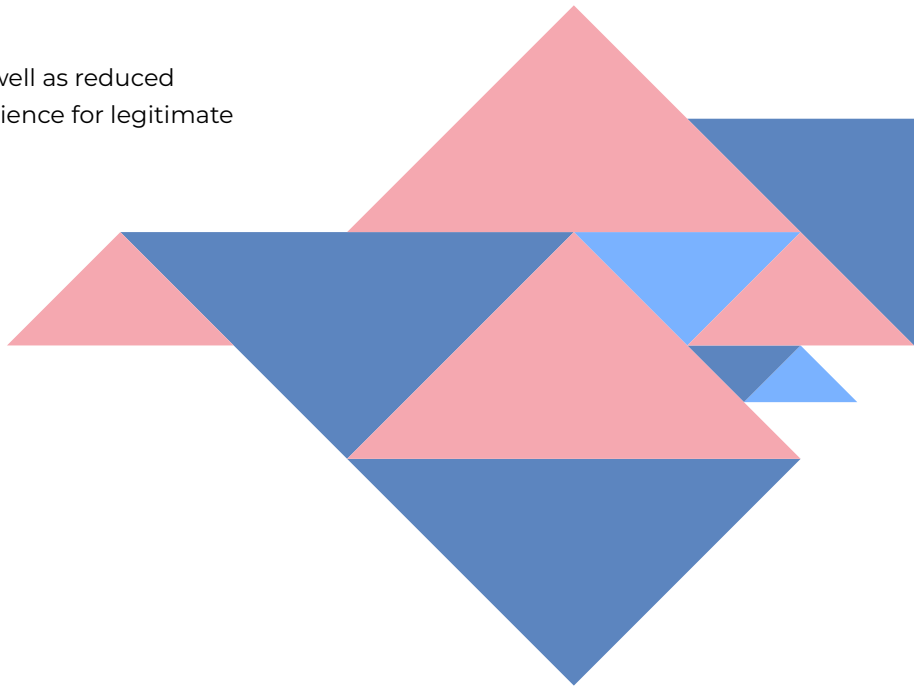
In both scenarios, the FI can identify the risk level of accepting a payment and releasing the customer's line of credit, reducing their exposure to losses while streamlining the customer experience.

Increase operational efficiency and maintain regulatory compliance

Employees at FIs are experiencing overwhelming workloads and process inefficiencies because of the time spent investigating fraud cases. By implementing a predictive intelligence tool like Payment Chek®, banks and credit unions can focus their resources on truly high-risk cases while simultaneously identifying low-risk transactions that don't require their time or resources.

Implementing Payment Chek® can also reduce the costs associated with compliance to KYC and AML laws, as well as help FIs maintain compliance with the Nacha Web Debit Account Validation Rule.

All of this can add up to major savings for FIs, as well as reduced workloads for employees, and an improved experience for legitimate customers—a worthwhile investment that pays dividends in the future.



CLICK HERE TO LEARN MORE

Conclusion

As new payments fraud attacks intensify and new tactics emerge, it's more critical than ever for FIs to share information and utilize predictive intelligence solutions to mitigate financial losses and protect customers.

Offering faster payments options has become table stakes for FIs to remain competitive and provide an exceptional customer experience. But with liability for losses from scams shifting heavily to FIs, and criminals constantly pivoting to exploit any gap in the system, banks and credit unions must invest in the predictive intelligence tools required to mitigate the impact of these fraudulent activities.

The good news is, with predictive intelligence solutions like **Payment Chek®**, FIs have been able to identify billions in high-risk credit card payments and prevent millions in potential losses.

LET'S DISCUSS

how *Payment Chek®* Service can enhance and fortify your payments fraud prevention strategy.

Complete the contact form at the bottom of the Payment Chek® page and an Early Warning representative will get in touch.

Sources

1 Datos Insights, Trends in Fraud for 2024 and Beyond, 2024
2 Association for Financial Professionals, 2024 AFP® Payments Fraud and Control Survey, 2024
3 Association for Financial Professionals, 2024 AFP® Payments Fraud and Control Survey, 2024
4 Thomson Reuters, SARs and fraud in 2024: Expect more — lots more, 2024
5 Nacha, ACH Network Records Strong Growth, 2024
6 Association for Financial Professionals, 2024 AFP® Payments Fraud and Control Survey, 2024
7 Federal Reserve, Commercial Checks Collected through the Federal Reserve--Quarterly Data, 2024
8 Association for Financial Professionals, 2024 AFP® Payments Fraud and Control Survey, 2024
9 Javelin, Identity Fraud Study: Resolving the Shattered Identity Crisis, April 2024
10 Datos Insights, Trends in Fraud for 2024 and Beyond, 2024

ABOUT EARLY WARNING SERVICES, LLC

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial system with cutting-edge fraud and payment solutions for more than three decades. We are also the company behind Zelle®, and the soon-to-launch Paze℠, a wallet that reimagines e-commerce payments. Early Warning partners with more than 2,500 banks and credit unions to increase access to financial services and products and protect financial transactions. Learn more at www.earlywarning.com and connect on LinkedIn.