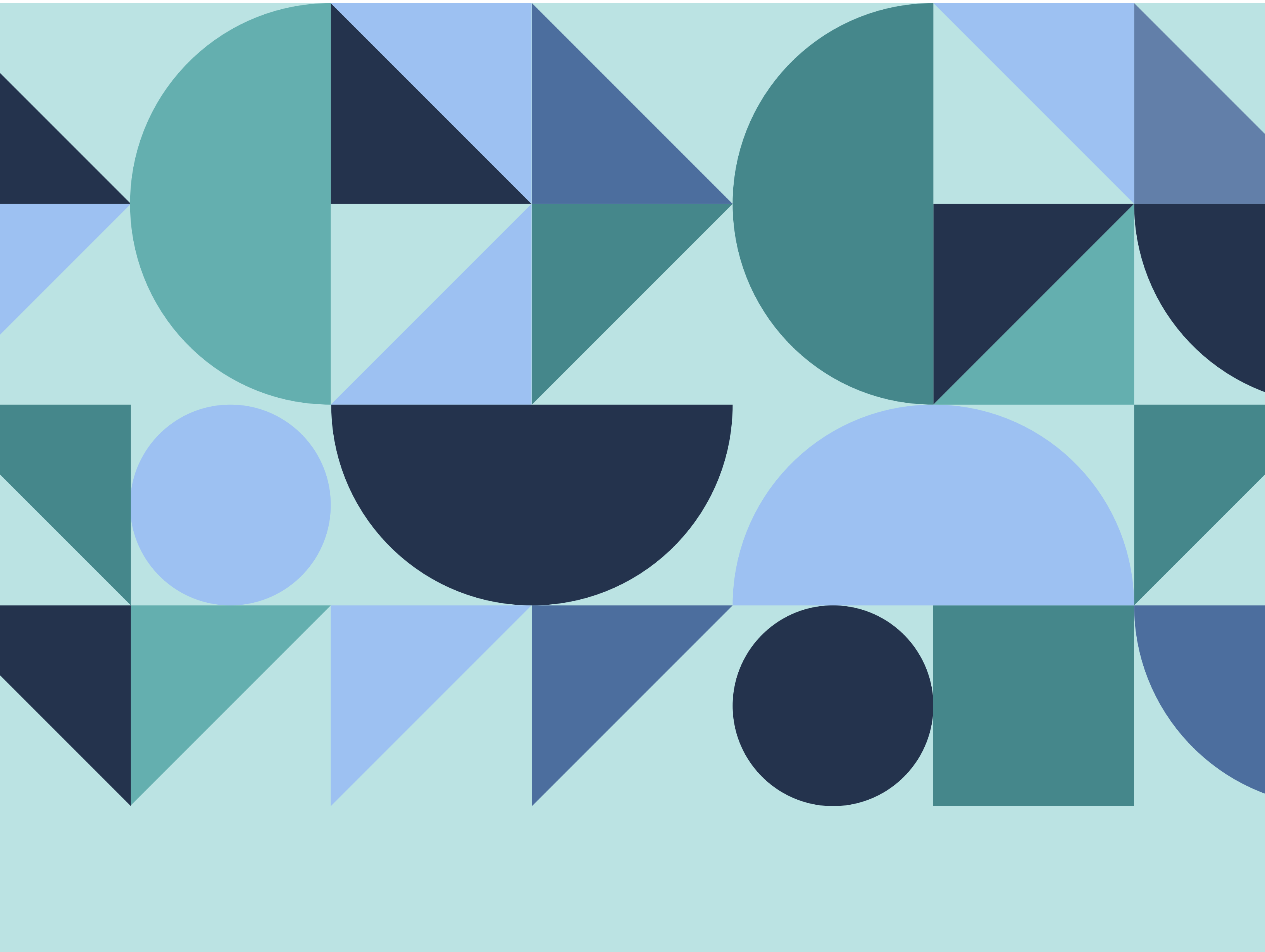
Early Warning®

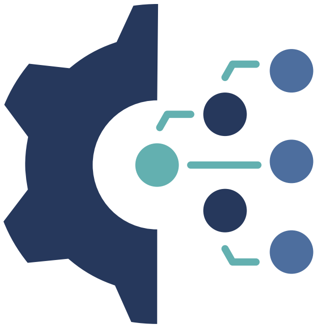
Detecting and Preventing Fraud with Data Analytics:

A Consortium Approach



Introduction

For financial institutions (FIs), staying ahead of fraud can feel like an uphill battle. As fraud evolves, FIs must update their systems with new tools that can protect against the latest trends.



Today, for example, the shift to digital banking, along with new technologies like generative AI, is spurring new fraud tactics that exploit weaknesses in traditional fraud management systems.

5%

Suspicious Activity Report filings—one of the most accurate measures of financial fraud—rose 5% in 2023,[1] and the upward trend is expected to continue.

To protect against growing losses, many FIs are investing in solutions that use data analytics for detecting and preventing fraud. **That's a good start.**

But when banks and credit unions only have access to data from their own institution, they only see a slice of a consumer's banking history and behavior. For data analytics to be an effective fraud prevention tool, the data itself must not only be timely and accurate; it must also be comprehensive.

In this guide, we explore the challenges FIs are facing in the fight against fraud, how fraud management has evolved, and why many FIs are embracing a data sharing approach.

Common fraud types are being perpetrated in brand new ways.

According to a 2024 Datos Insights report, check fraud and synthetic identity application fraud show significant increases, with 66% and 62% of FIs reporting rises in these areas year-over-year, respectively.[2]

Various fraud types, like check fraud, ACH fraud and synthetic identity fraud, are nothing new. But the tools and technologies criminals are using to perpetrate it are evolving, making the fraud harder for FIs to detect and prevent. Here are some examples:

66%

in check fraud

62%

in synthetic identity application

Check fraud:

Check fraud: Check fraud remains one of the most common fraud types, with 65% of organizations affected in 2023.[3] In recent years, crime rings have been targeting the U.S. mail service to steal checks in bulk. And they're using new technologies to wash and alter checks, making the bad checks nearly impossible to detect. What's more, once criminals have their hands on stolen checks, they can use the account information to produce high-quality counterfeit checks quickly and in greater quantities.

ACH fraud:

In 2024, 36 percent of FIs reported a year-over-year increase in ACH fraud.[4] And ACH fraud is continuing to rise as criminals develop new ways to exploit faster payment technologies. ACH credits, for example, have surpassed wires as the most vulnerable payment type for business email compromise (BEC), which impacted 63 percent of organizations in 2023.[5]

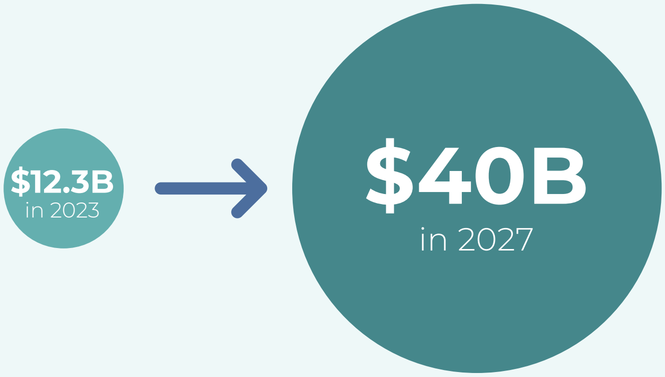
Synthetic identity fraud:

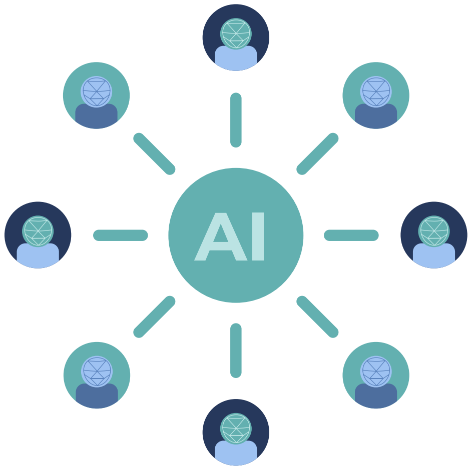
Synthetic identity fraud is notoriously difficult to detect and prevent. Widespread data breaches have made consumers' personally identifiable information (PII) easily available to bad actors. Now, criminals are exploiting new technologies to manufacture fake identities much faster and cheaper than ever before. Indeed, 62 percent of FIs say synthetic identity fraud is increasing.[6]

Generative AI has the potential to spur greater fraud growth.

Generative AI, the new kid on the AI block, is creating a stir across industries as a potentially revolutionary technology. Unfortunately, generative AI has the potential to revolutionize the fraud industry, too. By making it easier and cheaper for criminals to operate, it lowers the barrier to entry for more bad actors.

Estimates suggest that generative AI could lead to fraud losses of up to **$40 billion by 2027**, up from $12.3 billion in 2023.[7]





Generative AI is perceived as a major emerging threat, with 93% of financial institutions expressing concern about defending against AI-powered attacks.[8]

Identity verification is one of the areas being hardest hit by criminal use of generative AI. Here are a couple examples:

- **Deep fakes:** Using generative AI, bad actors can generate highly believable videos and voices and use them to impersonate individuals in real-time—making identity verification a major challenge.
- **Synthetic identities:** By handling time-consuming and complex creative tasks in seconds, generative AI empowers criminals to produce fake identities on a massive scale. Synthetic identities were already a growing problem. Generative AI exacerbates the challenges.

It's important to note that generative AI is still an emerging technology. We don't know how quickly the technology will advance or how it will be used. But we know one thing for certain: criminals will move fast to exploit it.

Where are FIs investing to improve fraud management?

In the past, most FIs relied on reactive fraud solutions that aimed to lessen the impact and losses after the fraud occurred.

More recently, FIs shifted to a proactive approach, with a focus on using data analytics to detect and prevent fraud from happening in the first place. The problem with many data-driven solutions, however, is that they rely on business rules and binary decision models. The tools' inflexible nature creates two key problems: they can slow down customer experiences (and frustrate customers)—and they rely on overly rigid "yes/no" decisions that can stunt business growth. FIs are balancing fraud prevention with customer experience, with 88% agreeing that customer experience is equally important to fraud loss control.[9]

Today, FIs are investing in advanced technologies to more accurately detect and prevent fraud—including predictive analytics, AI and machine learning (ML).

71%

of FIs reported using AI and ML to combat fraud in 2024—up from 66% in 2023 and 34% in 2022.[10]

DIGITAL IDENTITY AUTHENTICATION

Top investment priorities aimed at preventing synthetic identity fraud focus on digital identity authentication (55% of FIs) and identity verification controls (43% of FIs), reflecting the critical nature of these defenses in the digital banking era.[11]

| www.earlywarning.com

CLICK HERE TO LEARN MORE

Consortium data sharing is gaining momentum (for good reason).

When it comes to detecting and preventing fraud with data analytics, there’s one important thing to remember: *No matter how advanced the technology is, the value of the output depends on the quality of the data inputs.*

As such, many FIs are turning to consortium data sharing to maximize the value of their data-driven fraud controls. Tools that combine shared banking data with advanced analytics can better identify deviations from typical behaviors—and provide more accurate alerts.

No matter how advanced the technology is, the value of the output depends on the quality of the data inputs.

Early Warning customers benefit from consortium data sharing.

At Early Warning, our give-to-get model offers a prime example of how FIs can benefit from consortium data sharing.

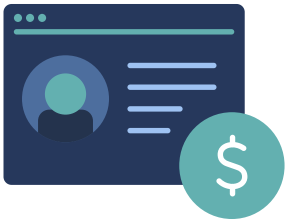
Depending on the product and services Early Warning customers use, they may gain actionable insights into approximately 90% of U.S. banking consumer identities.[12]

Thousands of FIs contribute data to our National Shared Database$^{\text{SM}}$ on a regular basis. In return, they get access to a holistic ecosystem of products and services to detect and prevent fraud in real-time.

CLICK HERE TO LEARN MORE

How to use Early Warning fraud solutions as an end-to-end package

EXAMPLE A:



NEW ACCOUNT OPENINGS

Access to the National Shared Database^{SM} fuels our data-driven solutions, giving FIs a transparent view of an applicant's account history and behavior.

When a consumer applies for a new account, the FI can verify the person's identity, determine their level of risk—and validate that they are the true owner of the funding account. Various fraud controls work together, in real-time, to ensure a secure and efficient onboarding process.

At the point of account application, FIs receive real-time risk scores and attributes, which they can use to make well-informed account opening decisions. Attributes supplement scores to provide a more nuanced view into an applicant's risk, including:

- Number of fraud records contributed for the individual
- Number of open or closed accounts
- Average number of days accounts have been open
- Number of accounts in a high-risk status
- Number of returns within the last 180 days

2023

Early Warning by the numbers:[13]

39 million

Helped the U.S. financial system prevent identity fraud by issuing over 39 million identity verification transactions.

83 million

Helped U.S. financial institutions reduce fraud exposure and open accounts with confidence by screening 83M new account applications.

$13 million

FIs receiving First-Party Fraud Scores were alerted to an average of $13M in total potential fraud loss.

CLICK HERE TO LEARN MORE

USE CASE:

1 The consumer is ready to open a new bank account and shares their information through the FIs application system

2 Early Warning accesses the National Shared Database^{SM} and runs advanced analytics, providing the FI with deep data intelligence:

   a. Verify Identity determines the likelihood the consumer is who they say they are

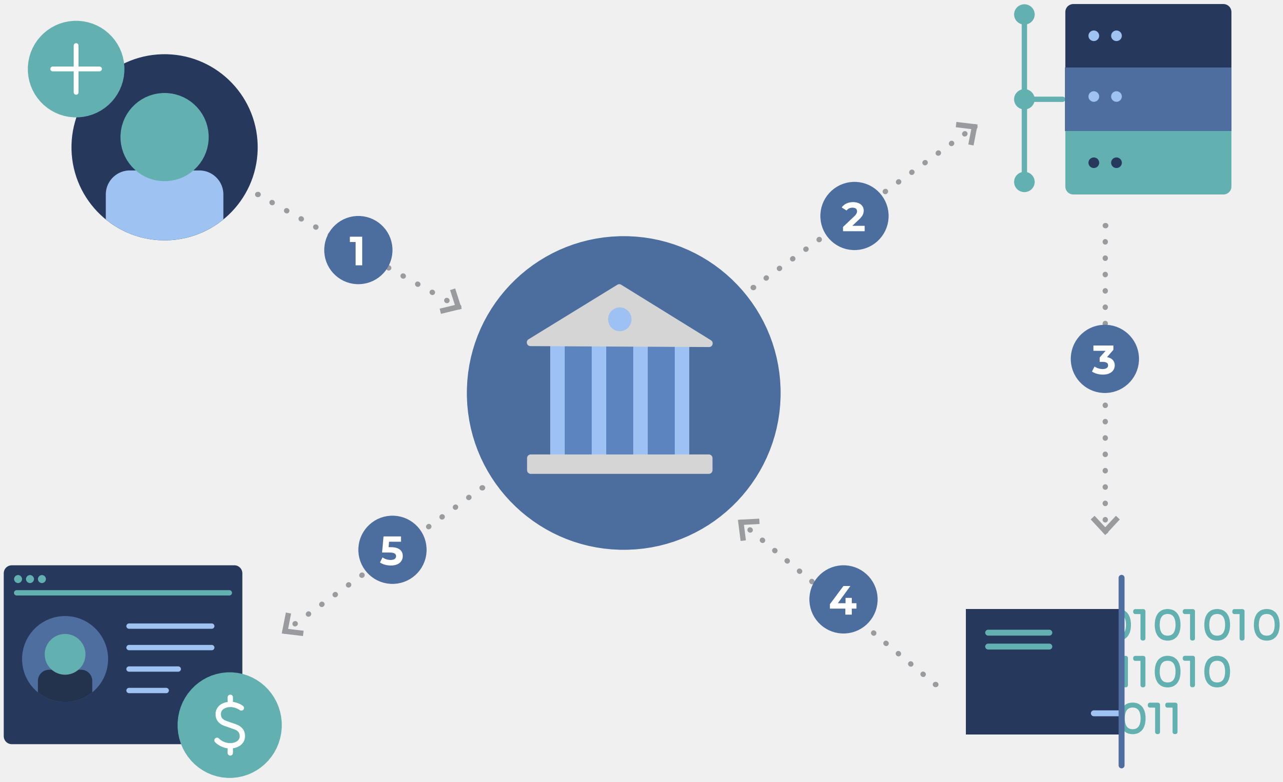
   b. Predict New Account Risk determines the likelihood that the consumer's account will be closed within nine months due to first-party fraud or account mismanagement

3 The account is approved, and customer makes an ACH deposit to fund the account

4 FI receives a real-time response from Deposit Chek® with Account Owner Authentication (AOA)—validating account ownership and alerting any high-risk deposits

5 Customer's deposit goes through—and the new account is open and funded

Real-time screening across deposit channels can reduce unnecessary holds on new accounts funded by external checks or ACH, making funds available to your customers sooner.



CLICK HERE TO LEARN MORE

EXAMPLE B:

PAYMENTS

Backed by the intelligence of the banking community, our product ecosystem protects against fraud at every point where money moves.

> In 2023, Early Warning alerted financial intuitions about $11M in payments that were going to accounts whose ownership information failed Payment Chek® verification.[13]

> Two billion items were analyzed through Deposit Chek® in 2023, alerting banks and credit unions to high-risk deposits and saving $1.76 billion in potential fraud loss.[14]

2023
Early Warning
by the numbers:

$11 million
ownership information failed Payment Chek® verification

$2 billion
items were analyzed through Deposit Chek®

USE CASE:

A financial institution with 5 million deposit accounts can expect to save $29M in annual fraud loss with Deposit Chek®.[15]

Responses include:

STATUS VERIFICATION

DUPLICATE ITEMS

STOP PAYMENTS

HIGH-RISK ITEMS

COUNTERFEIT ITEMS

TREASURY HIGH-RISK ITEMS

CLICK HERE TO LEARN MORE

The power of the network: Early Warning is uniquely positioned to help banks and credit unions thrive

For 35 years, we've been behind the scenes on many everyday banking interactions, from account openings to P2P payments to digital deposits. With our unique view into consumers' banking activity, Early Warning helps more than 2,500 banks and credit unions protect transactions and access the modern products their customers want.

We continue to innovate across three key areas:

Fraud prevention: As the Trusted Custodian® of the National Shared DatabaseSM, we connect critical data across thousands of banks and credit unions. In 2024 alone, Early Warning screened more than $11 trillion in payments and deposits to help prevent $3 billion in fraud.[15]

Moving money: We launched Zelle® to address the need for fast and convenient money movement in the US. In 2024, more than $1 trillion moved across the Zelle Network®.[16] Not in the Zelle Network® yet? Don't miss out on providing your customers with the experience they want.

Digital checkout: PazeSMis a new reimagined online checkout solution that banks and credit unions offer to consumers and merchants, combining all eligible credit and debit cards into a single wallet and eliminating manual card entry.technologies to more accurately detect and prevent fraud—including predictive analytics, AI and machine learning (ML).

To learn more about how your institution can use the power of the network to get ahead of [17]fraud, read the report: Consortium Data Sharing: A Valuable Tool in Fighting Fraud and Abuse.

LEARN MORE

about how to use consortium data to reduce fraud-without disrupting the customer experience.

Sources

1 SARs and fraud in 2024: Expect more — lots more, Thomsen Reuters, April 2024
2 Datos Insights, Nov. 2024
3 2024 AFP Payments Fraud and Control Survey Report, Association for Financial Professionals, 2024
4 Trust in the Digital Age of Financial Services: Preparing for Tomorrow's Fraud Threats Today, Datos Insights, Nov. 2024
5 2024 AFP Payments Fraud and Control Survey Report, Association for Financial Professionals, 2024
6 Navigating Synthetic Identity Fraud: Trends, Challenges, and Countermeasures in Banking, IDC, May 2024
7 Deepfake banking and AI fraud risk | Deloitte Insights, Deloitte, May 2024
8 Trust in the Digital Age of Financial Services: Preparing for Tomorrow's Fraud Threats Today, Datos Insights, Oct. 2024
9 Trust in the Digital Age of Financial Services: Preparing for Tomorrow's Fraud Threats Today, Datos Insights, Oct. 2024
10 Seven in 10 Financial Institutions Use AI and ML to Combat Fraud, PYMNTS, March 2024
11 Trust in the Digital Age of Financial Services: Preparing for Tomorrow's Fraud Threats Today, Datos Insights, Oct. 2024
12 Early Warning report, 2025
13 Early Warning report, 2025
14 Early Warning report, 2025
15 Early Warning report, 2025
16 Zelle® Shatters Records with $1 Trillion Sent in a Single Year, Zelle, February 12, 2025

ABOUT EARLY WARNING

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial services ecosystem with cutting-edge fraud and payment solutions for more than three decades. Through unmatched network intelligence and partnerships with more than 2,500 bank and credit union brands, we increase access to financial services and products, and protect financial transactions. We are the company behind Zelle®, and Paze^{SM}, an online checkout solution. Learn more at www.earlywarning.com.