Early Warning®

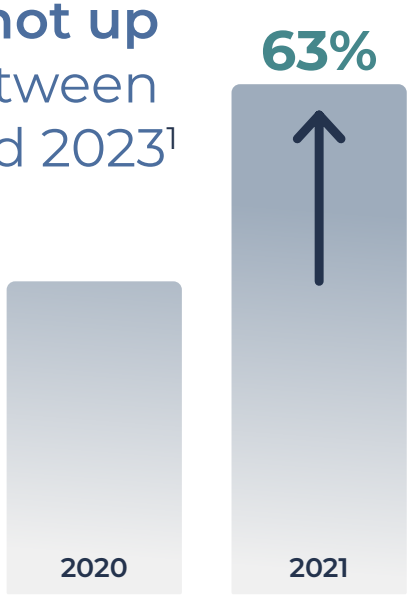
How to Prevent ACH Fraud: Four Best Practices for Financial Institutions

Introduction

Businesses and consumers have embraced ACH as a fast and easy way to send and receive money.

Unfortunately, thieves are exploiting these faster transactions to commit faster crimes. In recent years, ACH payments and deposits have become a prime target for theft.

ACH fraud losses **shot up by 47 percent** between 2021 and 2023[1]



...and the trend continues, 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]

This data reveals a growing threat that financial institutions cannot afford to ignore.

Use this guide to understand the basics of ACH, why ACH fraud is a growing concern, and how to prevent ACH fraud at your institution.

CLICK HERE TO LEARN MORE

What is ACH?

ACH refers to electronic transactions that move funds between two bank accounts.

ACH transfers are often used by businesses to pay employees via direct deposit or to pay vendors and suppliers for products. They're also frequently used by consumers to transfer money from one account to another, pay service providers, or pay taxes to the IRS.

In the U.S. all Electronic Fund Transfer (EFT) transactions are held in the Automated Clearing House (ACH) network until the money is cleared for transfer.

TERMINOLOGY

- **On-us (or internal) transactions** are fund transfers between two accounts at the same bank.
- **Off-us (or external)** transactions are fund transfers between accounts at two separate banks.
- **Originating Depository Financial Institutions (ODFIs)** are banks and credit unions that act as the middlemen between ACH Originators and the ACH network. Upon receiving instructions from an Originator, the ODFI initiates the ACH transaction.
- **Receiving Depository Financial Institutions (RDFIs)** are banks and credit unions that receive funds through the ACH network.

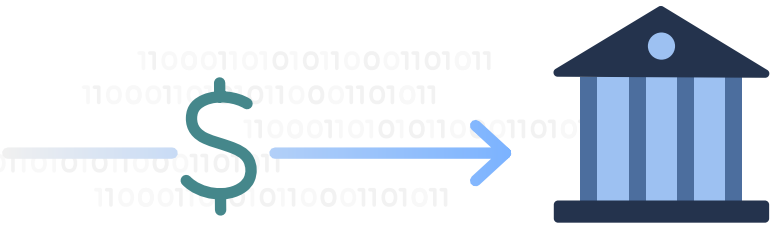
CLICK HERE TO LEARN MORE

What is ACH fraud?

ACH fraud refers to the theft of funds via unauthorized or illegitimate ACH transactions.

There are two main types of ACH fraud: ACH deposit fraud and ACH payments fraud.

ACH DEPOSIT FRAUD



ACH deposit fraud is similar to check fraud—in that the person initiating the deposit (the ACH credit) is the person committing the crime. The funds they are depositing are not coming from a legitimate account. New account funding is a common ACH deposit fraud tactic in which a bad actor funds a new account by initiating an unauthorized ACH credit from an account at one bank, then quickly withdraws the funds from the new account.

ACH PAYMENTS FRAUD

ACH payments fraud occurs when the person sending the money is committing the crime. The fraudster gains access to a compromised or fraudulent account and initiates 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.

CLICK HERE TO LEARN MORE

But if there's one thing we know about financial fraud, it's that new trends are always emerging. As banking technologies evolve, bad actors are always looking for new ways to steal from banks and their customers. Such is the case with ACH credit-push fraud.

ACH CREDIT-PUSH FRAUD

This type of fraud is a fast-growing threat. Like ACH deposit fraud, this type of theft makes use of ACH credits. The difference is that the ACH credit transactions are often authorized—albeit through trickery. Using sophisticated tactics like payroll impersonation, business email compromise schemes or fraudulent benefits claims, the criminal tricks the authorized account holder into sending them money using ACH credits.

Criminals typically target off-us ACH transactions when committing payments fraud because they know it's more difficult—and can take more time—for banks to assess the risk of an external account.

CLICK HERE TO LEARN MORE

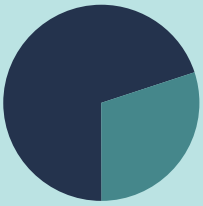
Why is ACH fraud so concerning?

ACH usage is growing fast—and fraudsters are cashing in.

With their sights set on faster payment technologies, criminals are continuing to develop new tools and tactics targeting ACH channels—making the risk of fraud loss greater than ever.

While payments fraud overall has been declining, fraud activity via ACH has become a growing concern.

In 2023, **33%** of financial institutions reported fraud activity via **ACH debits.**[2]



In 2023, ACH credits surpassed wires as the **most vulnerable payment type** for Business Email Compromise (BEC) fraud, with 47% of BEC attacks utilizing ACH credits.[2]

CLICK HERE TO LEARN MORE

How can your institution prevent ACH fraud?

To help safeguard your bank and your customers from ACH fraud losses, incorporate these four practices into your risk management strategy:

1

KEEP UP WITH FRAUD TRENDS

ACH fraud is continuing to evolve. Which means your fraud mitigation strategy must evolve, too. As new banking technologies emerge, educate yourself on the latest fraud trends and behaviors—and adjust your fraud detection and prevention approaches accordingly.

With some fraud trends, like synthetic identity fraud for example, criminals typically play the long game—nurturing fraudulent accounts for a year or more to embed themselves in the banking system.

But faster payment technologies are driving faster fraud behaviors. With ACH fraud, criminals are devising tactics to steal funds in near real-time. To combat today's fast fraud trends, it's critical to update your system with real-time ACH fraud controls.

2

EDUCATE YOUR CUSTOMERS

As you learn about new fraud trends, keep your customers in the loop. Continually educate and alert them to new fraud risks. Because your risk mitigation solution should work seamlessly behind-the-scenes, it's also important to inform your customers about the controls you have in place.

And remember: Winning the fight against fraud requires action on all fronts. Let your customers know what they can do to help mitigate their risk

CLICK HERE TO LEARN MORE

3

ADHERE TO INDUSTRY RULES AND STANDARDS

New and updated regulations are often put in place to address growing fraud trends. Following NACHA rules and KYC standards will help ensure your fraud mitigation strategy is up to date.

The NACHA WEB Debit Account Validation Rule, for example, helps combat ACH fraud by requiring an ACH Originator to validate a consumer's bank account information when initiating an ACH debit transaction.

Nacha developed a new Risk Management Framework to help combat the rise in ACH credit-push fraud. Many of these rules (which are slated to take effect in 2024) require financial institutions to strengthen their fraud detection and monitoring systems with respect to ACH transactions.

By putting account validation tools in place, you can help prevent ACH fraud—while making it easier for your corporate customers to stay compliant.

4

MAKE USE OF BIG DATA AND PREDICTIVE ANALYTICS

To stop ACH fraudsters in their tracks, you must be able to do two key things:

- Verify that the person making the transaction is an authorized account user
- Quickly assess the risk of both on-us and off-us transactions

You can do both those things by leveraging the power of big data analytics.

Early Warning® uses data from thousands of financial institutions to reliably assess fraud risk. Payment Chek®, for example, screens on-us an off-us ACH transactions against the Early Warning® database to answer crucial questions like:

- Is this person authorized to transact on the account?
- Is the account open and active?
- Is the account new?
- Is the account closed or overdrawn?
- Is the account a non-DDA account?
- Is the transaction high-risk?

CLICK HERE TO LEARN MORE

With access to timely data and real-time assessment tools, you can mitigate fraud risk—without disrupting the speed and convenience customers expect from your ACH services.

Learn more about how to prevent ACH fraud at your financial institution with real-time account validation.

LEARN MORE

about how Early Warning helps banks and credit unions prevent ACH fraud and protect customers.

Sources

1 Trends in Fraud for 2024 and Beyond, Datos Insights, Feb. 2024
2 Association for Financial Professionals, 2024 AFP® Payments Fraud and Control Survey, 2024

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 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.