Early Warning®

Protecting payments:

How real-time account validation enables safer transactions

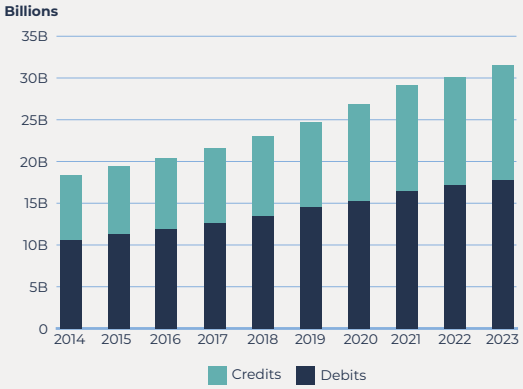
Introduction

The desire from both consumers and businesses for faster and easier electronic payments continues to drive an increase in ACH transactions year after year. Largely fueled by strong growth in same day ACH and business-to-business payments, the governing body of the ACH Network, Nacha, reported that total ACH transaction volume grew to 31.5 billion payments valued at $80.1 trillion in 2023.

This represents a **4.8% increase in transactions** over 2022 and an increase in **overall payment value of 4.4%**.[1]

ACH Network Growth Since 2014

ACH Payment Volume by Debits and Credits



While ACH payments facilitate fast and convenient transactions, a major plus for consumers and businesses, they have also attracted the attention of criminals seeing an opportunity to capitalize on this high-volume channel.

Bank transfers and payments fraud were the top payment methods most impacted by fraud in 2023 with losses amounting to $1.8 billion in 2023 according to the FTC.[2] As attempted payments fraud continues to rise and become more sophisticated, organizations and financial institutions face ever-increasing risk. And while fraud is a top concern for protecting against ACH losses, payments that are simply misdirected can also create significant losses of time and revenue and erode trust with customers.

Top Payment Methods and Losses

Banks and the treasury customers they serve, like insurance companies and government entities, need to know who they're transacting with so they can minimize losses from ACH fraud and misdirected payments, increase operational efficiency, and ensure compliance with Nacha rules.

How does ACH fraud happen?

ACH CREDIT-PUSH FRAUD

Business email compromise (BEC)

In a BEC scam, a fraudster gains access to or spoofs a legitimate email account of someone within a business organization, such as someone in upper management or the CEO. Then they manipulate an individual at that business into making a funds transfer, often by making the request seem urgent and important. Believing the request to be legitimate, the individual initiates an ACH transfer, directing the funds to an account controlled by the fraudster.

BEC scams are becoming more prevalent **with $2.9 billion in reported losses in 2023.**[3]

Cybercriminals can commandeer legitimate bank accounts by stealing a business or individual's valid login credentials. Once they have access to the account, they often direct the stolen funds to an account they control using an ACH or wire transfer.

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.

Misdirected payments

Erroneous payments aren't always part of nefarious or fraudulent activity. Misdirected payments, where the sending party makes a processing error when entering account information for the receiving party, are also a common and costly issue. Remediating these transactions can create a significant loss of time and revenue for financial institutions and organizations, and lead to a loss of trust and reputational damage with customers.

Account validation helps banks, credit unions, and organizations protect against ACH fraud

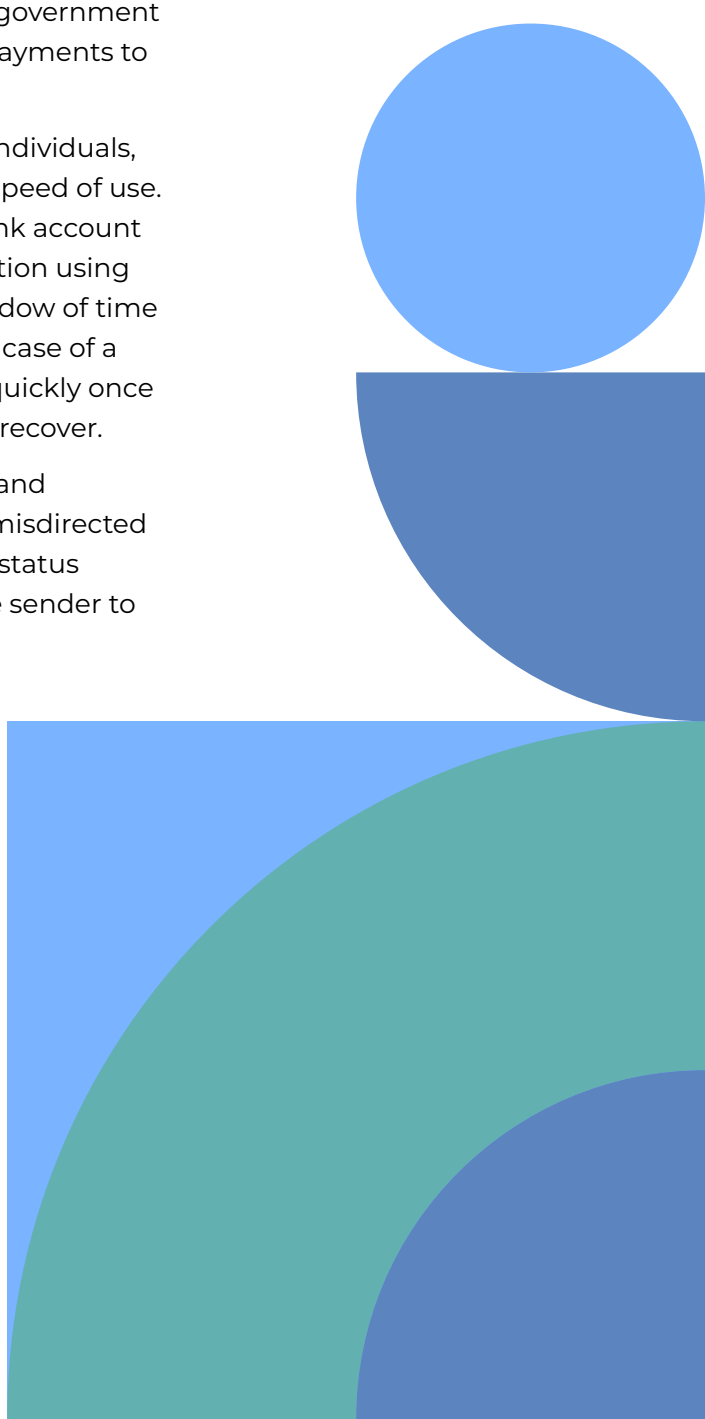
Account validation is a critical step for preventing fraudulent ACH transactions and can help raise the red flag on suspicious transactions before it's too late.

ACH and wire transfers are used to facilitate a broad range of everyday transactions such as businesses processing payroll or paying vendors, insurance companies making payouts on customer claims, government entities disbursing benefits funds, and customers making payments to their bank on loans or credit card statements.

These payment methods have become ubiquitous among individuals, businesses, and financial institutions due to their ease and speed of use. However, they carry some risk as anyone who knows the bank account information of an individual or business can make a transaction using the account, and financial institutions only have a small window of time to reverse a funds transfer once it has been executed. In the case of a fraudulent transaction, criminals will often launder money quickly once it's been received, making it extremely difficult to track and recover.

Banks and credit unions, as well as corporate organizations and government entities, can minimize the risk of fraud and/or misdirected payments by validating an account's authorized owner and status before sending a payment (e.g., wire or ACH). This allows the sender to confirm that the person they're intending to transact with is in fact the owner of the receiving account, and that the account is currently open.

Because validating an account prior to sending an ACH or wire transfer is so effective in minimizing fraud as well as the risk of misdirected payments, Nacha has mandated that originators of ACH payments conduct account validation the first time an account is used. This is known as the Nacha WEB Debit rule.



Choosing the right account validation method for your organization

There are several methods of validating an external account before an ACH or wire transaction is initiated. **Understanding the options for validating accounts will help you find the right solution for your organization**.

Micro deposits

A micro deposit is a small transaction, typically under $1, sent to an account via ACH to verify the account's ownership and information. While micro deposits offer a fairly easy way for financial institutions and organizations to verify a customer's account, there are several drawbacks including the fact that it's often a multi-day process, adding delays for customers, as well as the fact that fraudsters often already have access to the account.

Credential login

A credential login takes a basic login request using an email address and password and checks that the credentials provided are valid. This is another relatively easy method of account validation from the FI or organization's side, but one that adds an additional step for the customer. It's also susceptible to fraud because criminals have often obtained access to the account by stealing the individual's logon credentials.

Mailing voided checks

Customers can validate account ownership in the form of mailing a voided check to the FI or organization they want to transact with. However, this method is antiquated and cumbersome, leading to account abandonment and reduced revenue for the bank, credit union, or organization.

Real-time account validation

A real-time account validation method authenticates accounts using consortium data. The process is seamless and invisible to the customer and fast and easy for the bank, credit union, or organization.

Get ahead of fraud with real-time account validation:

HOW IT WORKS

Real-time passive account validation works behind the scenes to confirm that the person or organization receiving funds is the owner of the account and confirms the status of the account (i.e. open, closed, overdrawn).

Here's a real-world example of how it works:

Alex's washing machine leaks while he's away at work one day, causing a flood in his home. He makes a claim with his insurance provider, SafeHome, to repair the flooring, and chooses an ACH transfer to have the funds sent straight to his bank account for immediate access.

Now it's up to SafeHome to ensure that Alex's account is open and valid, and that he is actually the account owner.

SafeHome uses Verify Account from Early Warning to confirm that the account belongs to Alex and that he is authorized to transact on it—in real-time. Alex's account is verified and SafeHome issues the ACH credit.

With fast and frictionless account validation, Alex doesn't have to wait for a check to be mailed and can quickly receive his funds, allowing him to make his home comfortable again in no time.

EXAMPLE PROCESS:

Step 1
A customer makes a claim with their insurance provider.

Step 2
A customer chooses an ACH transfer

Step 3
SafeHome uses Verify Account from Early Warning for real-time verification

Step 4
Customer's account is verified and issued the ACH credit

Enable seamless, secure, and swift payments with Verify Account

Verify Account authenticates account ownership and external account status before an ACH or wire transfer is sent. Using this service, banks, credit unions, corporate organizations, and government entities can mitigate potential fraud by preventing funds from being sent to unauthorized accounts.

It leverages data from thousands of banks contributed to the National Shared Database℠ to verify the current account status, and checks whether a customer's personal information is a match with the authorized account owner and authorized signer. Organizations can quickly and confidently mitigate transaction fraud and determine whether an account is open and in good standing with real-time validation of user-provided accounts.

In 2023, Verify Account screened **$13.5 billion in outbound transactions**, preventing **$900 million from being sent to unauthorized accounts** and **preventing $56 million in possible fraud.**

WHAT IS THE *NATIONAL SHARED DATABASE*℠?

The *National Shared Database*℠ is a consortium-fueled data set used to power predictive data models from Early Warning®. More than 2,500 institutions regularly contribute data on their customers' account history and banking behaviors into this resource, helping to increase our coverage and strengthen our machine-learning capabilities.

As the Trusted Custodian® of the *National Shared Database*℠, Early Warning® receives deposit performance data from[4]:

697 million
participant/scored accounts

631 million
account owners

10.4 billion
annual transactions

Use Verify Account to:

Accurately disburse funds

This inquiry-based, real-time solution quickly validates account ownership without introducing friction to the customer, so you can be confident you're paying the right person.

Reduce fraud loss

Access to up-to-date and accurate account intelligence lets you better detect transaction fraud and reduce errors in your Payables and Receivables process.

Comply with Nacha rules

Verify Account complies with the enhanced WEB Debit Account Validation rule which requires ACH originators to use a commercially reasonable fraudulent transaction detection system.

Increase operational efficiency

Reduce the time and resources spent on rectifying misdirected payments.

LEARN MORE

about how real-time account validation can protect your bank, credit union, or organization

Sources

1. Nacha, *ACH Network Value and Volume Statistics*, 2023
2. The Federal Trade Commission, *As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public*, 2023
3. Federal Bureau of Investigation, *Internet Crime Report 2023*, 2023
4. Early Warning National Shared Database℠ Report December 2023

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.