



# ... Faster Payments Are Driving New Fraud Trends

**ESSENTIAL ELEMENTS OF A MODERN  
PAYMENTS FRAUD MITIGATION STRATEGY**

February 2023

# ••• New payment technologies bring new fraud tactics.

New and emerging banking technologies like same-day ACH offer speed and convenience for consumers.

They also open the door to new fraud risks.

Seeing a lucrative opportunity for theft, criminals are devising new tools for attacking modern payment systems.

## Common payments fraud tactics include:



### Check fraud (in person and digital)

- Counterfeit checks
- Forged or altered checks



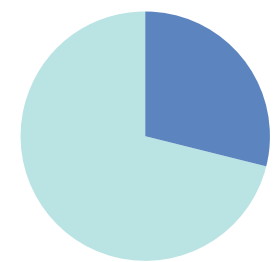
### ACH fraud (off-us ACH transactions)

- Credit card payments
- Loan payments
- Mortgage payments



# ••• The risk of payments fraud is greater than ever.

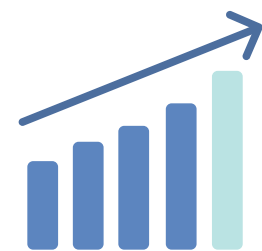
ACH fraud is on the rise—and check fraud is an enduring trend.



71% of organizations were victims of payments fraud attacks/attempts in 2021



In 2021, ACH debits were the second-most popular payment method targeted by fraudsters—second only to checks



The percentage of fraud activity via ACH debits has been increasing gradually—from 33% in 2019 to 34% in 2020 to 37% in 2021\*

A rise in unauthorized transactions results in higher costs associated with non-sufficient funds (NSF) and administrative returns.

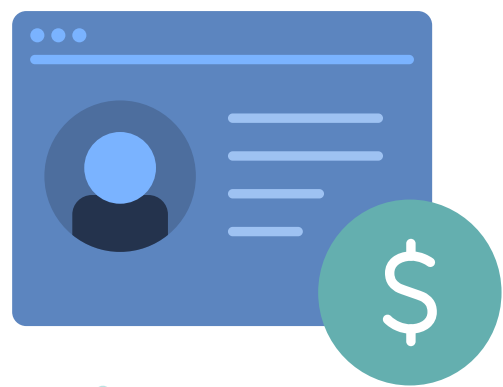
\* 2022 AFP® Payments Fraud and Control Survey, AFP®



# ••• Is it time to modernize your payments fraud mitigation strategy?

As transactions accelerate, you need real-time tools that can identify a potentially risky payment—before the transaction goes through.

You must be able to answer questions like:



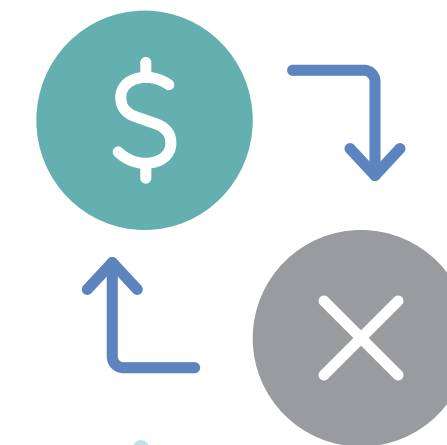
Does the external (off-us) payment account exist?



Is this person authorized to transact on the account?



Is the account open and in good standing?



What is the likelihood of the payment being returned?





A successful payments fraud mitigation strategy must keep up with industry changes.



# Customer expectations are growing.

New and emerging banking technologies like same-day ACH offer speed and convenience for consumers.

They also open the door to new fraud risks.

Seeing a lucrative opportunity for theft, criminals are devising new tools for attacking modern payment systems.



## ••• Security regulations are evolving.

To combat evolving ACH fraud threats, Nacha introduced the WEB Debit Rule—which requires businesses to validate a consumer's bank account information when initiating an ACH transaction.

For the bank receiving an ACH payment, verifying account ownership adds a valuable layer of protection against fraud.





# Verify Payment Risk

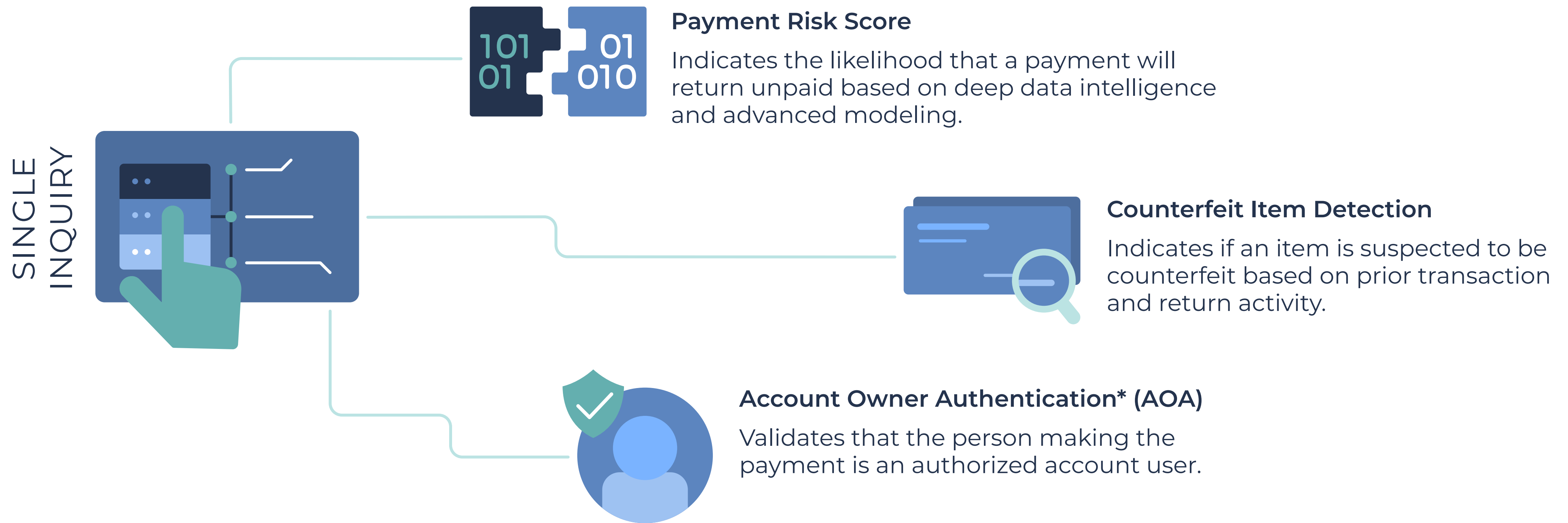
(formerly known as Real-time *Payment Chek*<sup>®</sup> Service)

**IDENTIFY HIGH-RISK TRANSACTIONS IN  
REAL TIME**





# ••• Confidently assess payment risk with a single inquiry.



\* AOA is available within **Verify Payment Risk** for an additional fee.

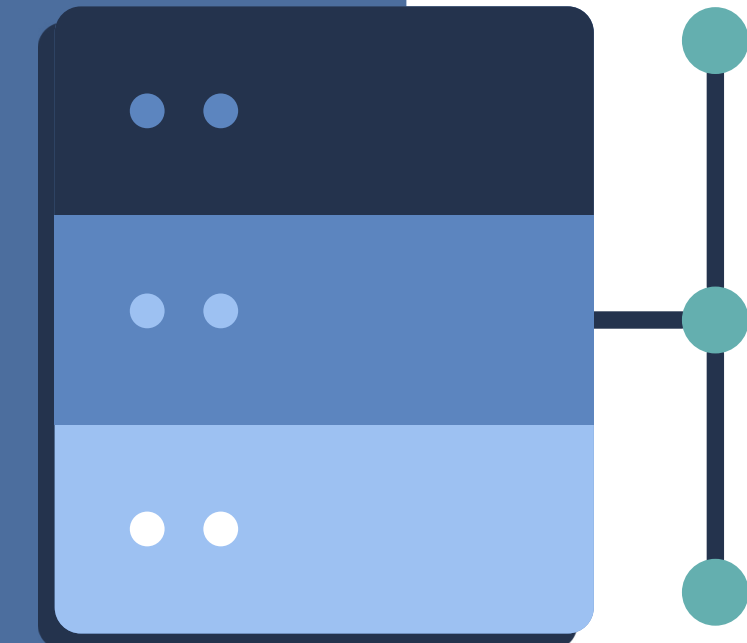


# ••• Leverage the power of big data analytics.

Early Warning<sup>®</sup> screens off-us payments against its *National Shared Database*<sup>SM</sup> resource to provide unrivaled insights into the risk associated with a customer's external account.

## *National Shared Database*<sup>SM</sup> Resource

- The Trusted Custodian<sup>®</sup> Role of Early Warning – June 2022
- Real-time access to data from more than 2,500 financial institutions



# How Verify Payment Risk works



1. A customer sends a payment to your institution from an external (off-us) bank account



2. You submit an account inquiry to Early Warning in real time



3. Early Warning checks the external account information against its *National Shared Database*<sup>SM</sup> resource and responds with insight on:

- Account type and status
- Account ownership (when optional AOA service is requested)
- Payment risk score



4. You make an informed decision about accepting/rejecting the payment based on the **Verify Payment Risk** response and your own risk tolerance





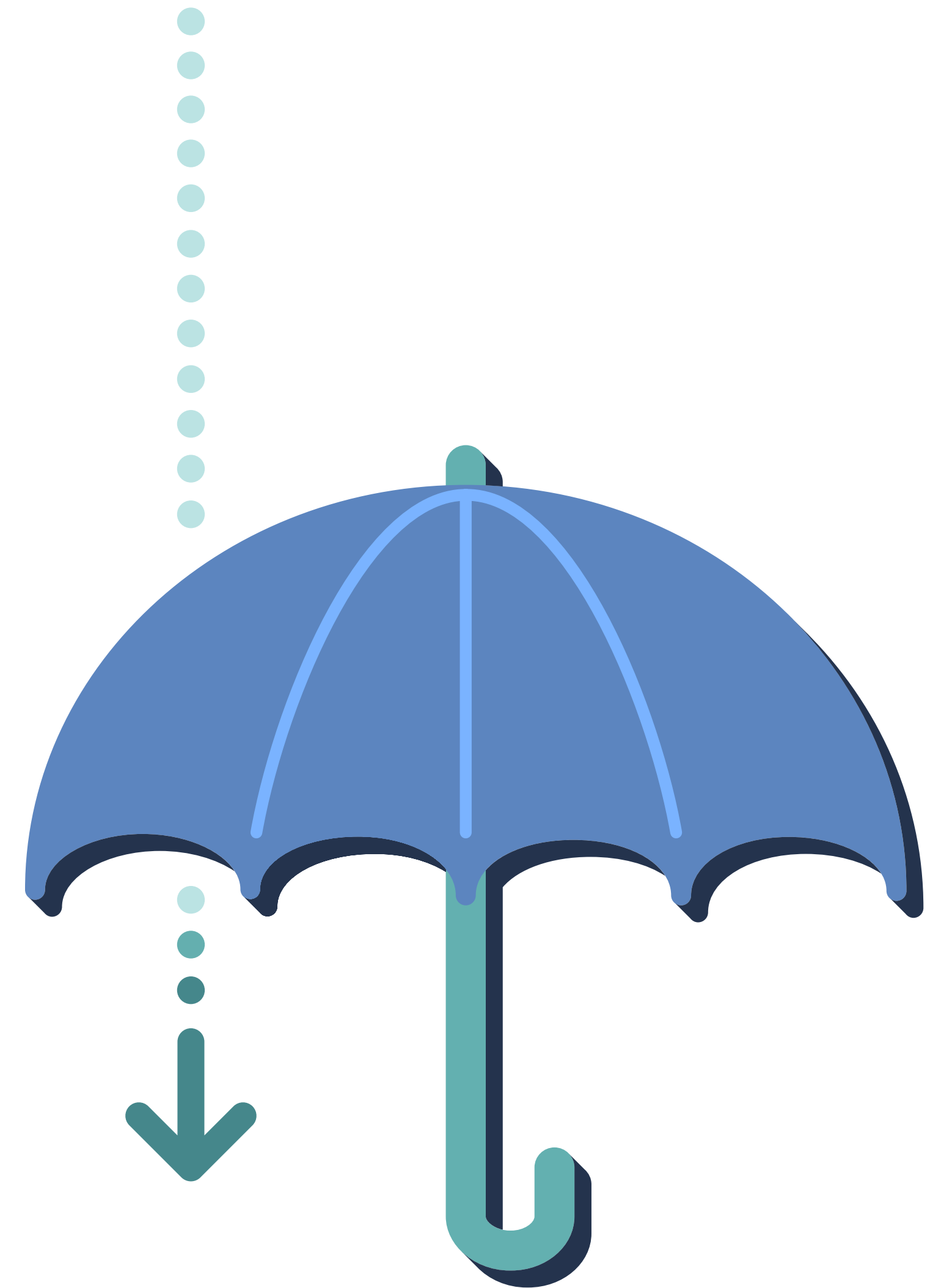
# How **Verify Payment Risk** can help your organization



# 1 Reduce losses due to payments fraud.

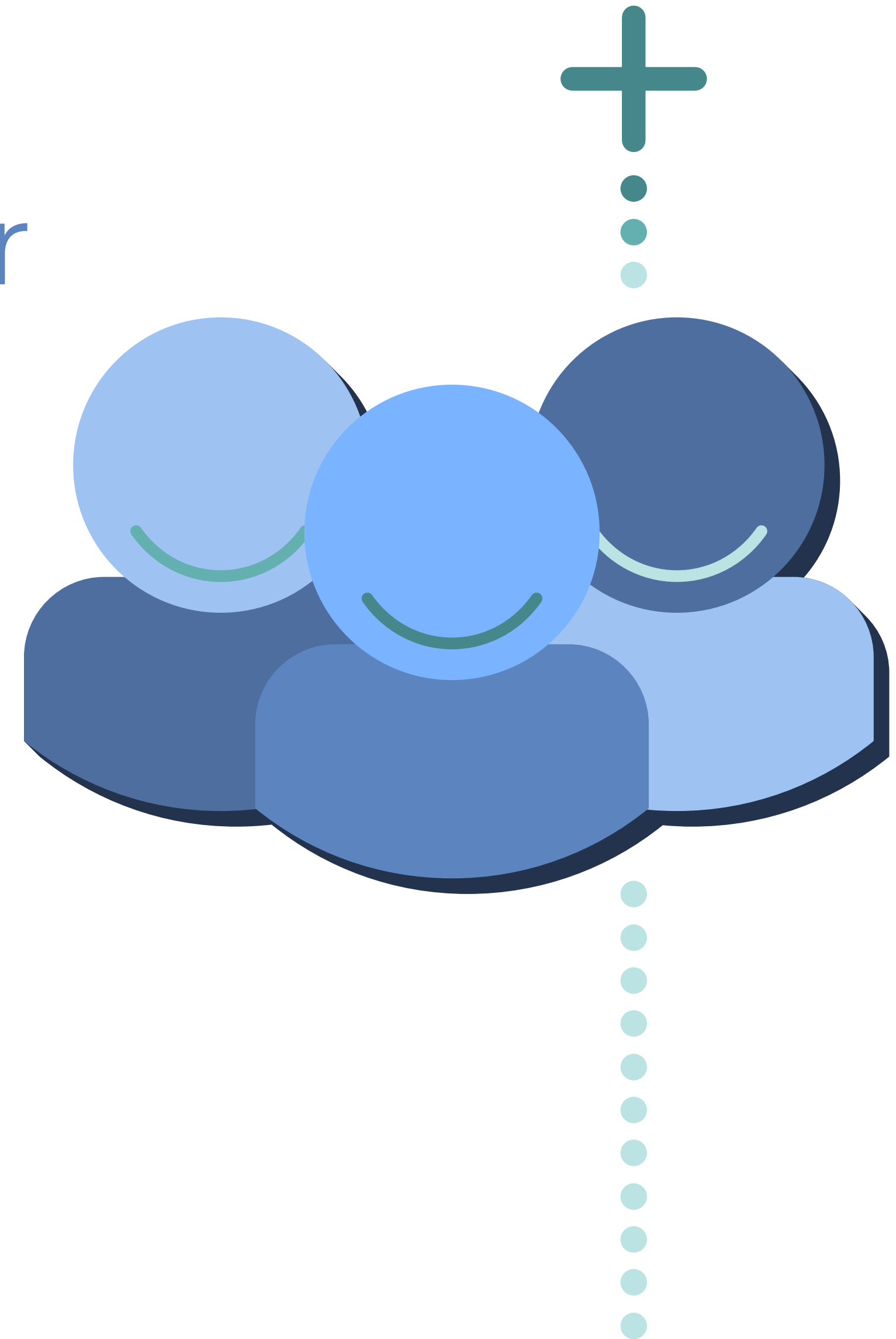
Reduce incoming non-sufficient funds (NSF) returns and validate outbound wires with:

- Point of presentment payment screening
- External account ownership verification
- External account status confirmation



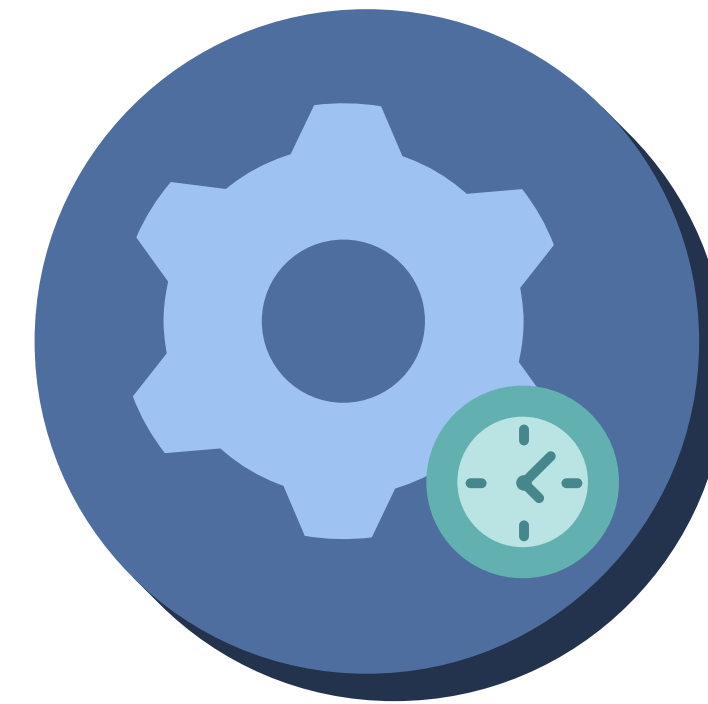
# 2 Improve the customer experience.

Ensure a seamless and consistent customer transaction experience across channels—with real-time insights into payment risk.



# 3 Balance risk, efficiency and compliance.

Stay compliant with Nacha's WEB Debit Account Validation Rule while configuring the capability's business logic to align with your own risk tolerance.





Can Early Warning help you enhance and strengthen your payments fraud mitigation strategy?

[LEARN MORE](#)





## ••• About Early Warning<sup>®</sup>

Early Warning is a fintech company owned by seven of the country's largest banks. For more than three decades, our identity, risk and payment solutions have been empowering financial institutions to make confident decisions, enable payments and mitigate fraud. Today, Early Warning is best known as the owner and operator of the Zelle Network<sup>®</sup>, a financial services network focused on transforming payment experiences.

With a partner like Early Warning, FIs are empowered with an accurate, comprehensive solution that:

- ✓ Provides breadth and depth of deposit data, enabling a holistic view of a consumer's banking behavior
- ✓ Leverages real-time, predictive analytics that enable better-informed decisions
- ✓ Ensures faster decisions and reduced friction which translates to a better customer experience





Early Warning<sup>®</sup>