Nacha®

A New Risk Management Framework for the Era of Credit-Push Fraud

A Nacha Report, September 2022

Table of Contents

Executive Summary

Fraud keeps changing. As it does, participants in the payments system need to understand and adapt to emerging fraud scenarios and develop counterstrategies to help protect their customers and themselves.

Nacha's previous risk management strategies for the ACH Network have focused on protecting consumers, organizations, and their account-holding financial institutions from fraud due to unauthorized debits that pull money from their accounts. Now, however, the most significant fraud threats to bank account holders involve fraud and scams that result in money being sent out of their accounts using credit payments, including ACH credits, wires, cards, and other instant and digital payments.

This new Risk Management Framework identifies current fraud threats that result in credit-push payments through the ACH Network and other payment rails, highlights significant challenges that credit-push fraud scenarios present, and identifies opportunities to improve fraud detection and prevention, and aid in the recovery of funds. As a new risk management strategy, the Framework is intended to bring the ACH Network and the broader payments community together to address an emerging and important area of need, and to provide an overarching direction for new initiatives, guidance, rules and industry tools.

While Nacha's role in the payments industry is governance of the ACH Network, credit-push frauds are broader than ACH payments. The strategies, themes, and opportunities identified here are applicable to other payment systems and methods, and the payments industry should work together across different payment methods.

As the Framework demonstrates, a new way of thinking about fraud detection, prevention and recovery is needed, as is a cultural change in the industry about fraud information sharing. All participants in the payment system, whether the ACH Network or elsewhere, have roles to play in working together to combat fraud.

Signed,

Jane Larimer
President and CEO
Nacha

Introduction

Previous ACH risk management strategies[1] largely focused on debit origination to mitigate the impact of unauthorized debits on consumers, businesses and other organizations, and their Receiving Depository Financial Institutions (RDFIs). Debit fraud schemes by their nature tend to be concentrated and identifiable at the point of origination; mitigation and prevention measures are best implemented at that point of origination. While risk from debit fraud scenarios remains, the payments industry has developed and implemented rules, tools, and educational programs that are widely understood and deployed.

In the current environment, however, fraudsters increasingly make use of payments in which consumers, businesses, and other organizations send money out from their accounts. These payments are known as credit payments, or credit-push payments. Common examples of fraud scenarios that target credit-push payments are business email compromise, vendor impersonation, and payroll impersonation (see Page 7). These schemes largely rely on social engineering to induce action by the account owner to initiate a payment. In many cases the payment is knowingly sent and is therefore an authorized payment.[2]

According to the Association for Financial Professionals, business email compromise (BEC) is the most prevalent source of attempted and actual payments fraud experienced by businesses. The FBI's Internet Crime Complaint Center reported that in 2021 there were $2.4 billion in losses due to BEC-style frauds. Research by Nacha suggests these numbers are likely underreported and undercounted due to the difficulty of recovering funds even if reported, and to factors related to embarrassment or to the reputational risk of the victims.

As distinct from debit scenarios, success in a credit-push fraud scheme relies on access to an account at the receiving institution. Funds are directed to and concentrated in an account(s) controlled by the fraudster, and then are withdrawn or sent to accounts elsewhere, including outside the U.S. These receiving accounts are often newly opened or mule accounts with limited history and activity. In these types of cases, the receiving, account-holding institution often is in the best position to identify potentially fraudulent credit transactions posting to these accounts. In addressing credit-push frauds, receiving institutions should have an active role in fraud detection, prevention, and recovery.

Also distinct from debit scenarios, success in fighting credit-push frauds requires cooperation and information sharing among financial institutions and other stakeholders. Improved information sharing can counter fraud by improving awareness and understanding of fraud scenarios, enabling communication and recovery between parties regarding specific instances of fraud, and providing qualitative and quantitative data for organizations to use in benchmarking, pattern identification, and anomaly detection.

Nacha provides up-to-date information on current fraud threats, and develops tools, guidance, and sound business practices to improve fraud detection, fraud prevention, and recovery of funds.

Learn more about ACH risk management at nacha.org/content/risk-management

[1]2005 Strategy – A New Strategic ACH Rules Framework for Risk Mitigation in the 21st Century; and 2013 Risk Management Strategy.

[2]In the UK, this has been labeled Authorized Push Payment (APP) Fraud.

Methodology and Objectives

In 2022, Nacha undertook a fresh and holistic look at risk management for the ACH Network. Guided by the Board of Directors, Nacha utilized dialogue and input from a variety of sources: the Risk Management Advisory Group, the ACH Network Advisory Board (consisting of ACH Network end users and service providers), the Rules and Operations Committee, and the Nacha Direct membership. With ideas and direction from these sources, a third-party expert consultancy conducted in-depth interviews with financial institutions, businesses, and other industry stakeholders to test the overall direction of the framework and develop specific action items. The results form the basis of this new Risk Management Framework, with three overarching objectives:

1. **Increase awareness of fraud schemes that utilize credit-push payments;**
2. **Reduce the incidence of successful fraud attempts; and**
3. **Improve the recovery of funds after frauds have occurred.**

While Nacha's primary role in the payments system is governance of the ACH Network, the themes, objectives and opportunities described in this Framework are applicable to other payment methods and systems beyond ACH.

Areas of Focus and Opportunity

This Risk Management Framework identifies three areas of opportunity for the ACH Network and other payments participants to focus on in our efforts to combat credit-push frauds.

1. Defining the role of the receiving account-holding institution

The receiving institution is often considered a passive participant in the flow of a payment, responsible only for the timely, accurate posting of transactions. In credit-push fraud scenarios, though, the receiving institution may be in the best position to identify questionable or suspicious credit payments. Receiving institutions can and should take an active role in identifying fraud. New risk management guidance for receiving institutions can address inbound transaction monitoring standards, and sound business practices for controls on funds availability for potentially fraudulent transactions and accounts, including early access to funds. The industry then can consider whether this guidance should be adopted as new rules.

2. Enabling and providing information sharing among financial institutions

Greater and better information sharing among financial institutions can be used to counter fraud in multiple ways: improved dissemination and awareness of fraud scenarios; communication and collaboration between participants on specific instances of fraud; and qualitative and quantitative data sharing on fraud patterns. Improved communication and collaboration between financial institutions on specific instances of fraud could be achieved through Nacha's Risk Management Portal and ACH Contact Registry, and through other industry platforms or services.

Importantly, fraud information sharing works best when all financial institutions are active contributors to the effort instead of being passive recipients of information.

3. Expanding and improving end-user awareness and education

Reaching end users of the payment system and encouraging them to act is a persistent challenge. Better, more effective end-user education equips users to detect and prevent fraud on their own. The challenge is reaching customers before they experience fraud. Financial institutions often find that customers do not take the initiative to learn about fraud methods, adopt controls or preventive tools, or even access readily available internal information, until they have become a victim of fraud. Financial institutions, third parties and other stakeholders can implement new and innovative customer education programs, and provide fraud controls and prevention tools and services on an opt-out basis. Professional certification programs can expand to incorporate the themes and findings from this Framework.

Conclusion

As credit-push frauds emerge and persist, risk management in the ACH Network and other payment systems must adapt to address these new schemes and to assist in the recovery of funds. The three areas of focus for the 2022 Risk Management Framework will challenge the industry to change and cooperate. Enhanced industry guidelines and potential changes to the Nacha Operating Rules will ask receiving banks and credit unions to take a more active role in fraud prevention. Information and data sharing between and among financial institutions will require trust and cooperation. Effective end-user education will require new and innovative ways to reach the end users of the payment system. Working together within and beyond the ACH community, participants in the payment system all have roles to play in combatting fraud.

Understanding Fraud Scenarios that Use Credit-Push Payments

Business email compromise schemes occur when the legitimate email account of a business officer is either compromised or impersonated and used to order or request the transfer of funds. An employee transfers funds to the fraudster believing the order was from a reputable company email address owned by an officer with authority to make those orders. Business email compromise is classified as Relationship and Trust Fraud by the Federal Reserve's FraudClassifier Model because an authorized party was manipulated into initiating a payment.

Vendor impersonation fraud occurs when a business, public sector agency or organization receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The fraudster is paid by the business, agency, or organization when the real contractor submits an invoice for work done or goods sold. Public sector organizations are frequently targeted because contract information is often in the public record. Vendor impersonation fraud is classified as Relationship and Trust Fraud by the Federal Reserve's FraudClassifier Model because an authorized party was manipulated into initiating a payment.

Payroll impersonation fraud targets employees and human resources departments. A fraudster will impersonate an employee and contact the HR department directly or through the employer's payroll portal using stolen credentials. The fraudster requests to change the account where the employee's regular payroll is deposited. Once updated, the employer pays the fraudster rather than the employee. Payroll impersonation fraud is classified as Compromised Credentials or Impersonated Authorized Party depending on whether the fraudster uses stolen credentials to access the employer's HR portal or impersonates the employee when contacting the employer's HR department.

Account takeover fraud occurs when a fraudster obtains the credentials of a consumer or a business bank account and pushes credits to their own accounts. The fraudster is active in the victim's online bank account, knows the account balances, and can quickly deplete entire accounts. Account takeover fraud is classified as Compromised Credentials because an unauthorized party initiates payment using stolen credentials.

Federal Reserve FraudClassifier℠ Model

The Federal Reserve worked with the payments industry to create the FraudClassifier model to help organizations classify fraud consistently. Nacha participated in the development of the FraudClassifier model and encourages the model's use. The model supports a common fraud language across payment types and fraud methods that can help all parties work together to identify and fight fraud. Applying the model across organizations and the industry ensures greater consistency in fraud classification, more robust information, and better fraud tracking.

More information on the Federal Reserve FraudClassifier model can be found at:
https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

Learn more about ACH risk management at:
nacha.org/content/risk-management