TOWN HALL

FPC Town Hall: A New Risk Management Framework for the Era of Credit-Push Fraud

February 23, 2023

Welcome to our presenters!

Devon Marsh, APRP
Senior Director, ACH Network Administration
Nacha

Jordan Bennett, AAP, APRP
Senior Director, Network Risk Management
Nacha

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

Embracing Nacha's New Risk Management Framework

February 23, 2023

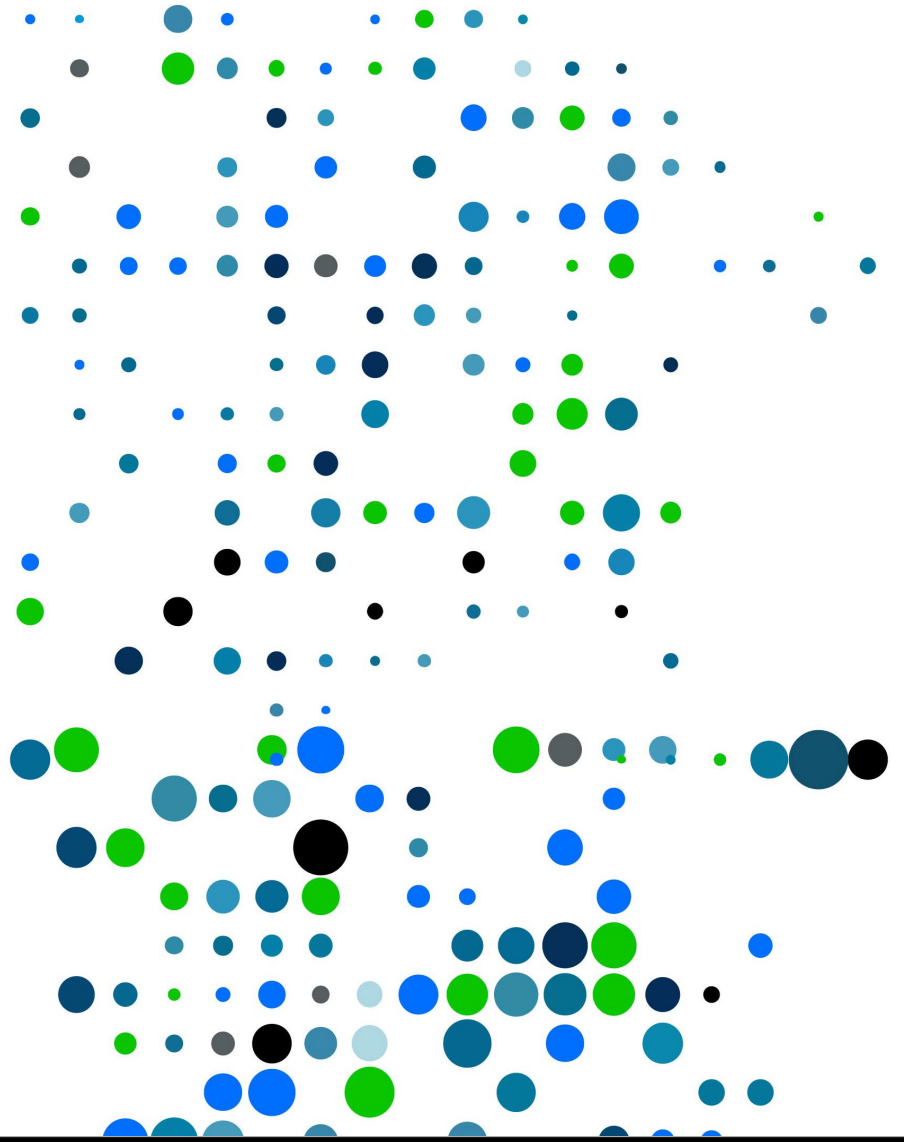
Devon Marsh, APRP
Senior Director, ACH Network Administration
dmarsh@nacha.org

Jordan Bennett, AAP, APRP
Senior Director, ACH Network Risk Management
jbennett@nacha.org

Why a New ACH Risk Management Framework?

Previous ACH risk management strategies were based on mitigating the impact of unauthorized debits on consumers and RDFIs:

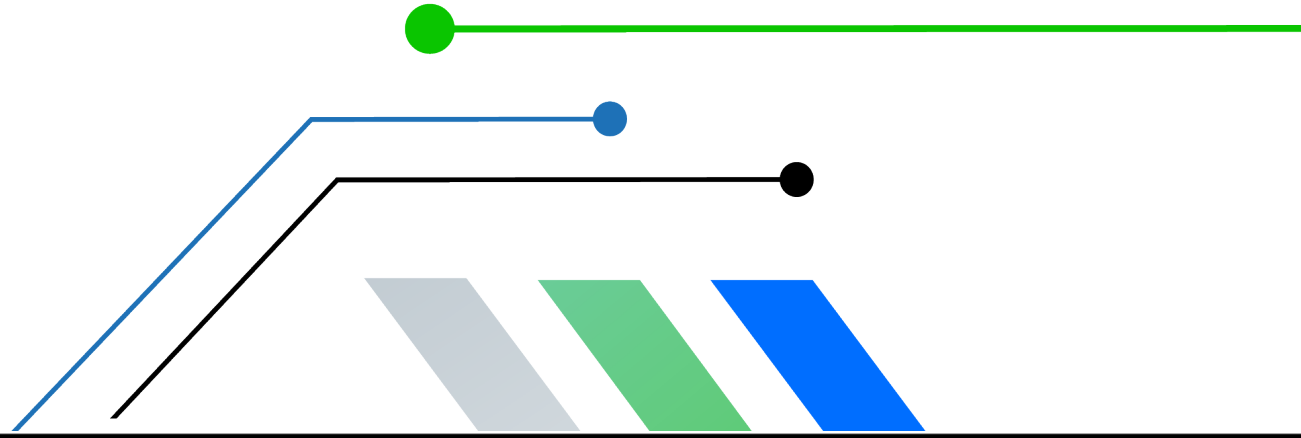
- 2005 Strategy – A New Strategic ACH Rules Framework for Risk Mitigation in the 21st Century (the "Two Sparrows" report).
  - "Primary goal to reduce the rate of unauthorized debits."
  - Primarily Rules focused.
- 2013 Risk Management Strategy.
  - Identified high-level themes relevant to risk management; and was primarily Rules focused.
  - Also primarily oriented around risks of consumer debit origination.



Why a New ACH Risk Management Framework?

These previous ACH risk management strategies and plans were intended to:

- Bring the ACH community together to address an emerging and important area of need.
  - The volume and rate of unauthorized debits were increasing.
- Provide an overarching guide to future Rules and other initiatives.
  - Recommendations and identification of priorities informed ongoing Rules and Operations Committee and Risk Management Advisory Group work.
  - Overall direction was established, even while annual plans evolved.
- Demonstrate effective self-governance.

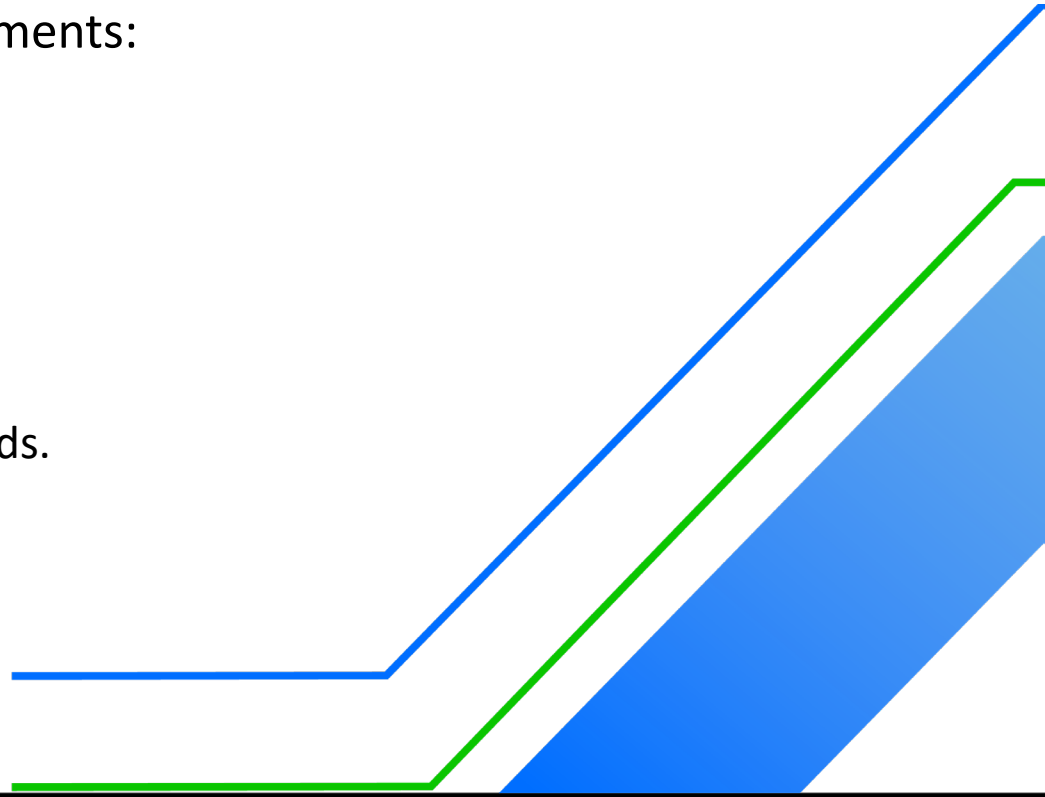


Why a New ACH Risk Management Framework?

More recently, there have been significant fraud scenarios affecting consumers, businesses and other organizations that make use of ACH credits and other “push” payments:

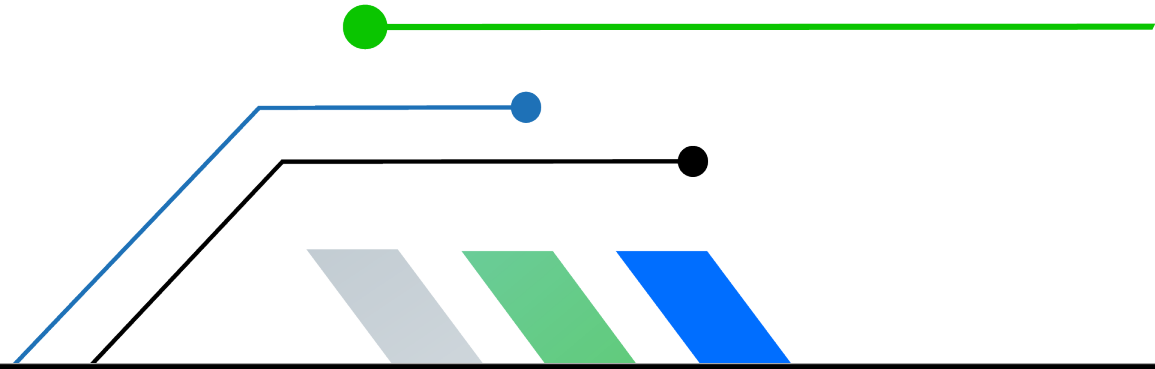
- Business email compromise (BEC).
- Vendor impersonations.
- Payroll impersonations.
- Account takeovers.
- Other impersonations (e.g., real estate settlement).
- Fraudulent claims for benefits – unemployment, PPP loans, tax refunds.
- Fraudulent use of micro-entries.
- Fraudulent inducements (e.g., romance scams; concert tickets).

These scenarios present some key differences from debit fraud.



Scope of BEC-type fraud and losses

- 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.

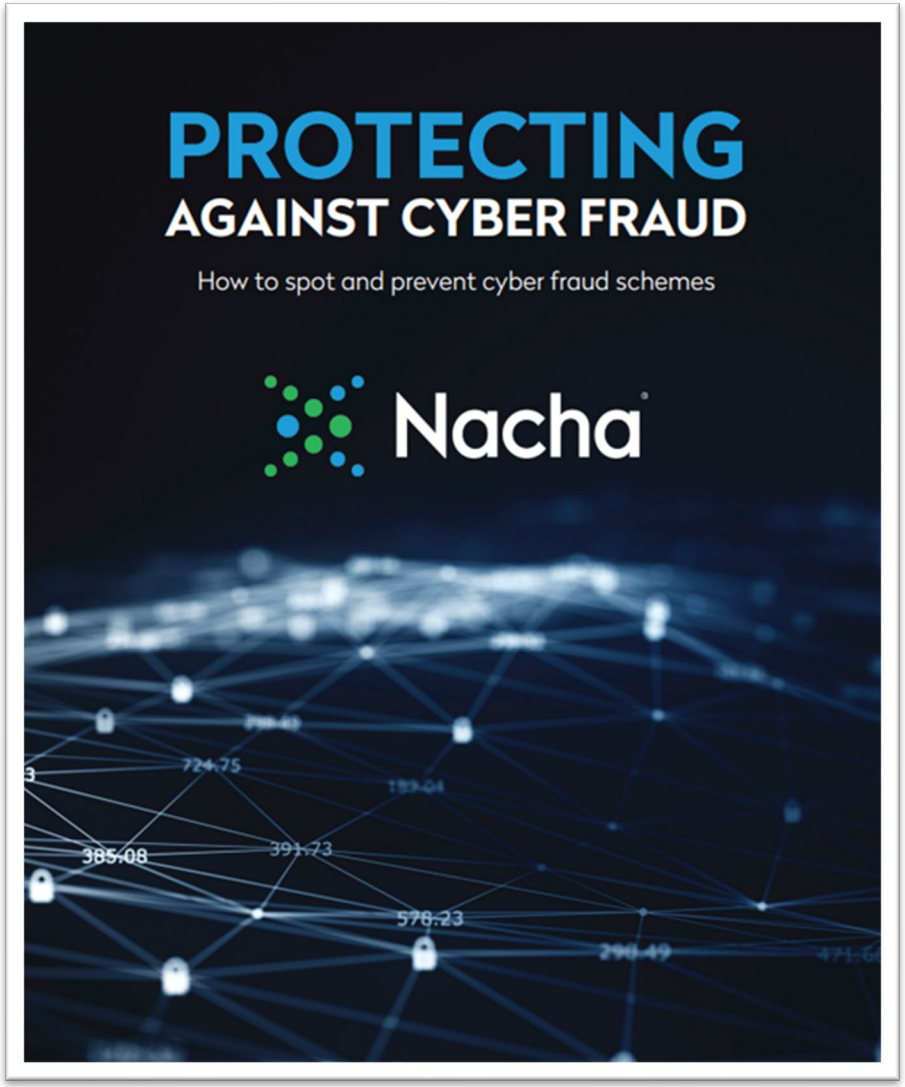


Protecting Against Cyber Fraud

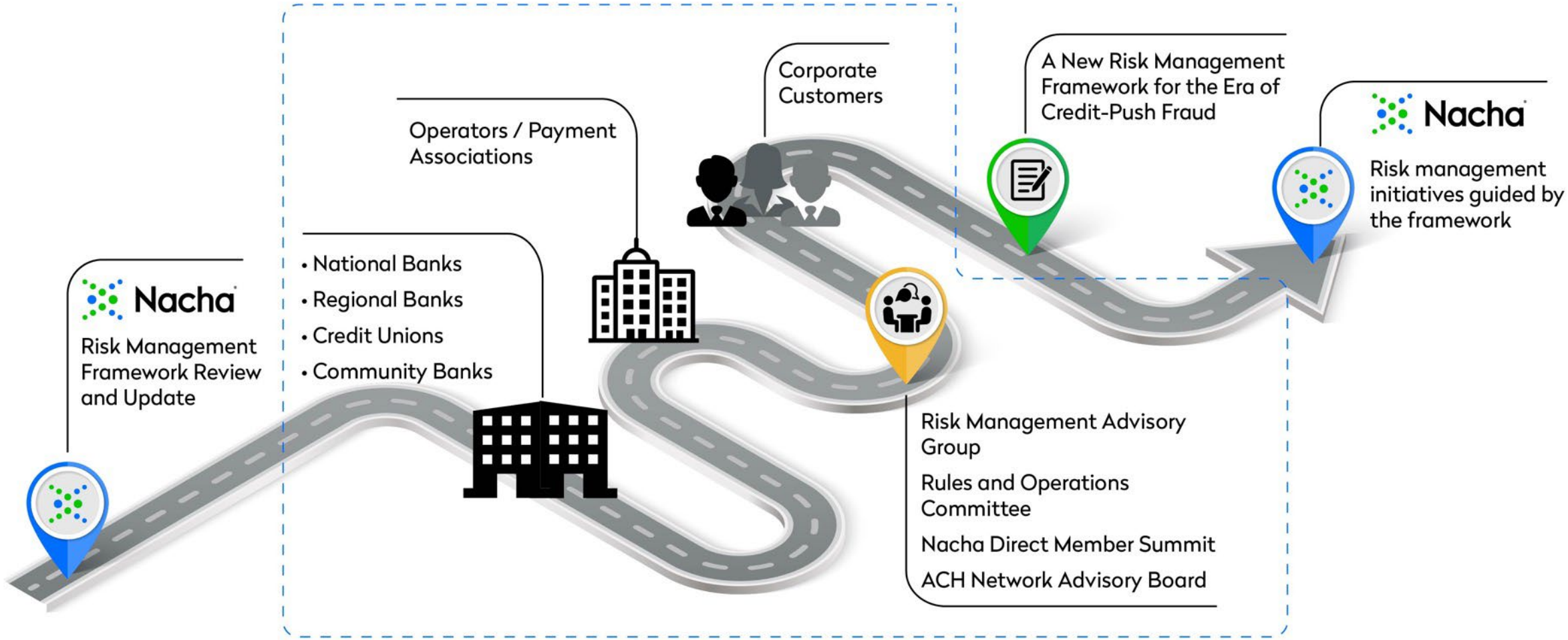
Nacha's e-booklet, *Protecting Against Cyber Fraud,* provides specific information and tips for ACH users to identify and defend against these types of frauds.

Download at:

https://www.nacha.org/sites/default/files/2021-10/Nacha_Fraud_Booklet_Updated_Oct_2021.pdf



Discussions with Participants



Framework Objectives

Participants encouraged Nacha to focus on three objectives:

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

Framework Launched

Released September 22, 2022

- https://www.nacha.org/content/risk-management.
- Nacha media release via multiple channels.
- Briefings to Nacha members.
- Introduction of initiatives into the ACH rulemaking process.
- Ongoing socialization with industry associations and institutions.

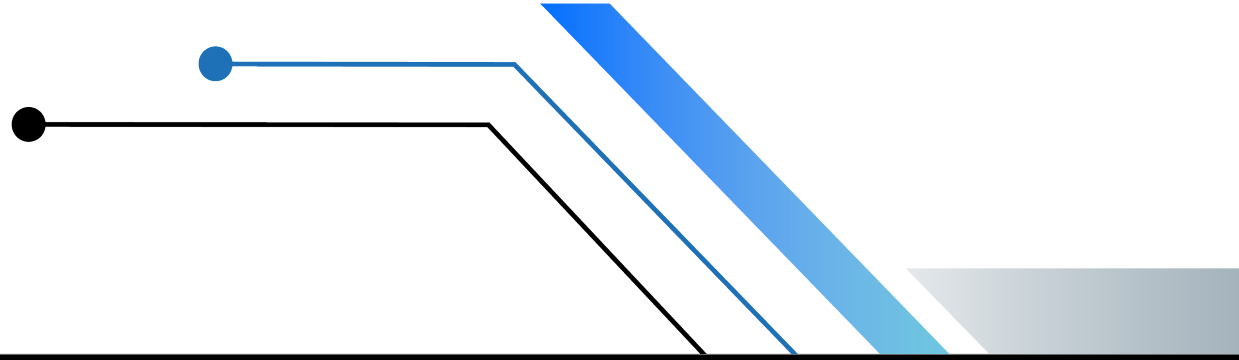
ACH Risk Management Framework – Major Themes

- Frauds that result in credit-push payments present some key differences from debit fraud:
  - They are not unique or specific to individual payment methods.
  - In many cases, the payments themselves are authorized.
  - Their success relies on the use of accounts at an RDFI(s).
    - New accounts / mule accounts.

ACH Risk Management Framework – Major Themes

- Credits and credit returns are not covered by the current Rules and risk framework for forward and return transaction monitoring, which covers only debits.
  - In many cases, there are no returns to monitor.

- Receiving FIs also are not covered by the current Rules and risk framework on transaction monitoring.



ACH Risk Management Framework – Major Themes

- RDFIs have a role to play in detecting, preventing and recovering from fraud that utilize ACH and other credits.
  - In some fraud scenarios, RDFIs may be in the best position to identify and stop fraud.
  - Early access to funds by RDFIs can be attractive to fraudsters.

ACH Risk Management Framework – Major Themes

- Information sharing
  - Financial institutions often need to contact each other for information and assistance.
  - General information on fraud scenarios.
  - Alert that there is a fraud happening.
  - Request or assistance with recovery of funds.
  - Leverage tools like the ACH Contact Registry to facilitate greater FI-to-FI contact .
  - Corporate end-users also express a desire and a need for fraud information sharing.

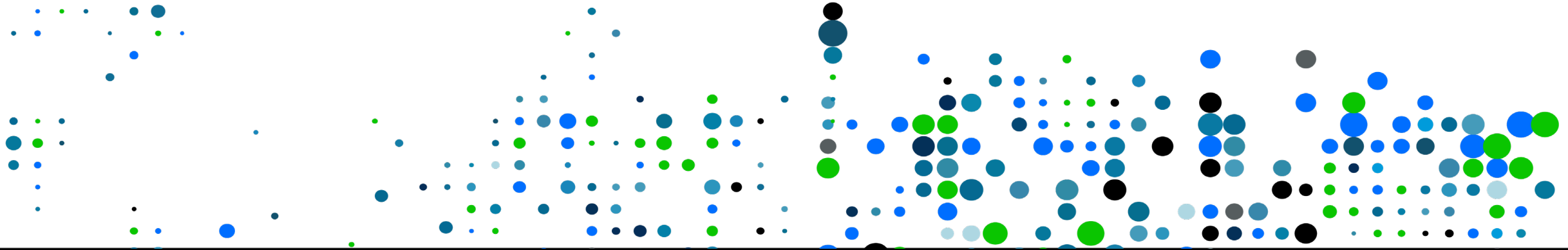
Framework Areas of Focus and Opportunity

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

Framework Areas of Focus and Opportunity

Enabling 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.
    - Qualitative and quantitative data sharing on fraud patterns.



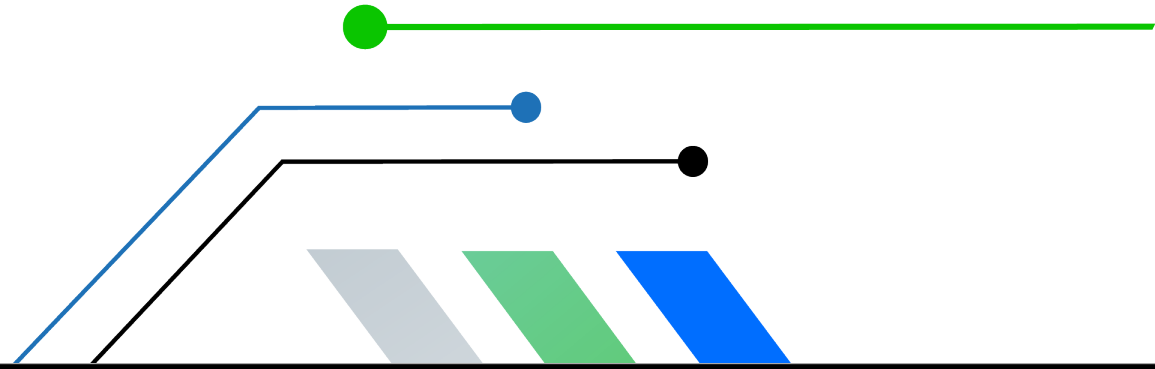
Framework Areas of Focus and Opportunity

Improving end-user awareness and education:

- Better, more effective end-user education equips users to detect and prevent fraud on their own.

Nacha Created End-User Education

- White label materials for FIs to incorporate into their messaging:
  - Sample email language.
  - Printable materials.
- First theme was Business Email Compromise in Q4 2022 followed by Romance Scams in Q1 2023:
  - Materials available .
  - FIs can use around the holidays to educate end-users.



All payments system participants have a role

Originators and Receivers:

- Report all instances of fraud to your financial institution or trusted 3rd party.
- Engage in end-user training.
- Adopt available fraud detection and prevention tools; don't wait until you are a victim.

ODFIs:

- Track proven and reported cases of fraud and provide benchmarking to originators.
- Expand information sharing with RDFIs.
- Invest in additional training and create incentives for originators to engage with training.
- Evaluate making certain fraud tools opt-out.
- Cross reference certain originations across gray list and flag transactions with destination accounts on gray list for further due diligence.

All payments system participants have a role

RDFIs:

- Implement enhanced monitoring and velocity checks.
  - Determine what transaction monitoring is already being done for AML.
- Potentially delay early funds availability and provide notice to originator in certain instances.
  - Enhanced KYC when providing early funds availability.
- Expand information sharing with ODFIs.
  - Notify ODFIs of accounts or transactions suspected of potential involvement in fraud.

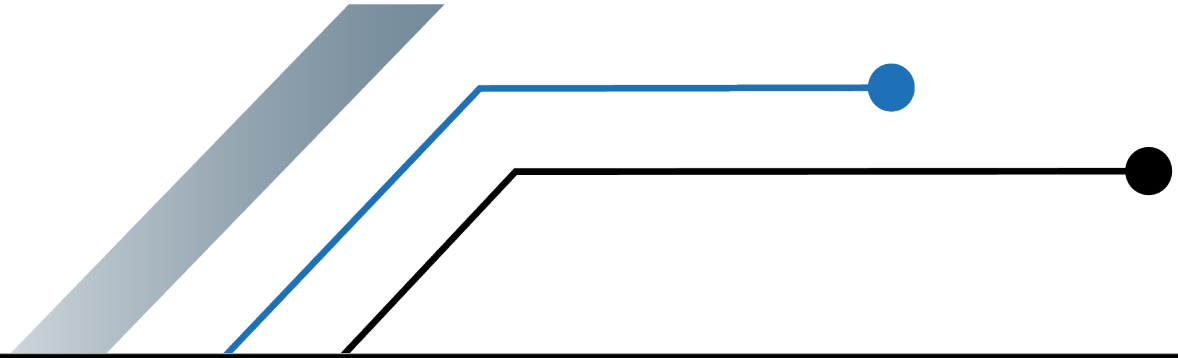
All payments system participants have a role

Operators and third-parties:

- Engage ODFIs / RDFIs in further study of the types of data which, if made available, would enable more effective fraud pattern research.

Regulators

- Provide clarity to financial institutions on the duty to act.
- Support financial institutions and provide safe harbor when acting in good faith.



All payments system participants have a role

Nacha:

- Provide clarity on responsibilities and expectations through the Guidelines and the Rule making process.
    - RDFI transaction monitoring.
    - Early funds availability.
    - Information sharing.
    - Suspected fraudulent item return code.
    - Payment field standardization for ease of identification and automated monitoring.
- Enhance communication tools in the Risk Management Portal.
    - Information Sharing.
    - Incident resolution.

The Risk Management Portal Incorporating New Ideas to Manage Risk

The need: means to communicate incidents of suspected ACH fraud and risk management issues with financial institutions in the ACH Network.

ACH Discussion Board in the Portal:

- New module in the Risk Management Portal.
- Accessible by all financial institutions registered in the Portal - currently more than 8,200 institutions.
- View and participate in posts by other financial institutions.
- Post information and receive feedback.
    - Financial institution users in the Portal total – approximately 28,000.
    - ACH Contact Registry - over 43,000 contacts.

The Risk Management Portal
Incorporating New Ideas to Manage Risk

Secure FI to FI Direct Messaging:

- Enhanced secure email module in the Risk Management Portal.
- Accessible by all financial institutions registered in the Portal.
- Send to and receive from direct messages (FI to FI).
    - Supported by information in ACH Contact Registry contacts and users registered in the Portal.
        - Financial institution users in the Portal total – approximately 28,000.
        - ACH Contact Registry - over 43,000 contacts.

Nacha's Implementation Progress

Risk Management Advisory Group (RMAG) Guidance:

- RMAG Offers Guidance for Risk-Based Controls to Address the Potential of Fraudsters Gaining Access to Illicit Funds | Nacha
- RMAG Guidance on ODFI Credit-Push Fraud Response Checklists | Nacha
- In the Fight Against Fraud, Nacha's RMAG Urges Information Sharing | Nacha

Rules and Operations Committee:

- The committee met in person in January 2023.
- Assessing potential topics for Rule making.

New threats require new ways of thinking about fraud detection, prevention, and recovery

- The ACH Network and other payments systems must adapt to address new schemes.
- The payments industry must change and cooperate in new ways.
- Receiving Banks and Credit Unions will take a more active role in fraud prevention.
- Effective education requires new and innovative ways to reach end users of the payments system.

Nacha Direct Member

Wrap Up

FPC Town Hall

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

The presentation materials and recording of today's FPC Town Hall will be available in our FPC Member Portal

www.fasterpaymentscouncil.org
memberservices@fasterpaymentscouncil.org