Next Generation Fraud Management in Treasury Services: Fraud Trends in Treasury and Business Account Fraud and Impact of New Nacha Rules on ACH Fraud

STOUT

Disclaimer

This presentation is for informational purposes only; it does not take into account any specific individual or entity's facts and circumstances. The presentation content does not constitute legal, financial, accounting, or other professional advice, and should not be relied upon by you or any third-party, including to operate or promote your business, secure financing or capital in any form, obtain any regulatory or governmental approvals, or otherwise be used in connection with procuring services or other benefits from any entity. Presenters assume no liability for viewers' use or use by any third-party of the information herein and please note, before making any decision or taking any action, you should consult with legal and professional advisers.

All opinions expressed by the presenters and in the materials are those of the authors and do not necessarily reflect the views of Stout Risius Ross, LLC, Stout Advisors SA, Stout Bluepeak Asia Ltd, Stout GmbH, MB e Associates S.r.l., Stout Park Ltd, Stout Capital, LLC.

Agenda

- Introduction
- Current Fraud Trends in Treasury
- New Nacha Rules on ACH Fraud
- Best Business Practices in Fraud Management
- Advanced Fraud Detection Technologies

Introduction

ACH Risk Management Topics Overview

Fraud monitoring by all parties in ACH except consumers

- ODFIs, Originators, Third-Parties
- RDFI monitoring of inbound ACH credits

Funds recovery tools

- Allowing RDFI returns for suspicious activity
- Clarifying ODFI's ability to request a return
- Exception to RDFIs' funds availability requirements

Standardized information

- Entry Descriptions – PAYROLL, PURCHASE

Written Statement of Unauthorized Debit (WSUD) processes

- Acknowledge ability of Receivers to claim unauthorized upon presentment
- Prompt return of debit after receipt of completed WSUD

Current Fraud Trends in Treasury

Current Fraud Trends

- **Generative AI:** Generative AI technology provides bad actors access to sophisticated tools to commit fraud

Examples of generative AI used for fraud:

- Synthetic identity fraud,
- Forged documents and financial statement manipulation,
- Deepfake fraud (e.g., image and video manipulation, human voice generation)

Current Fraud Trends

- **Business email compromise (BEC)** is a sophisticated phishing scam that targets businesses and individuals via email to access financial information or other sensitive data.

According to the FBI, there are five common BEC attack types:

- Data theft
- CEO fraud or whaling
- Email account compromise (EAC)
- Attorney impersonation
- False invoice scheme

Current Fraud Trends

- **One-time password (OTP) bots:** Some scammers use so-called OTP bots to trick people into sharing the authentication codes. The scammer might try to log in, prompting the bank to send you a one-time code. At the same time, the bot imitates the company and calls, texts or emails you asking for the code.
- **Cross Channel fraud:** refers to fraudulent activities that occur across multiple channels or platforms, involving the fraudulent use of various payment methods, accounts, or identities. It typically involves the exploitation of vulnerabilities within an interconnected ecosystem of online and offline channels.
- Theft from deposit accounts by way of multiple points of access whether branch, automated teller machine, call center, debit card, online banking, ACH or wire.

New Nacha Rules on ACH Fraud

Effective Dates for Rule Amendments

Date	Rule Amendments
October 1, 2024	Codifying Expanded Use of Return Reason Code R17 • Expanded Use of ODFI Request for Return/R06 • Additional Funds Availability Exceptions (for RDFIs) • Timing of Written Statement of Unauthorized Debit • RDFI Must Promptly Return Unauthorized Debit
March 20, 2026	Fraud Monitoring (by ODFIs) ▪ Fraud Monitoring (by [non-consumer] Originators, TPSPs, and TPSs with 2023 ▪ ACH origination volume of 6 million or greater) ▪ ACH Credit Monitoring by RDFIs (with 2023 ACH receipt volume of greater than 10 million) ▪ New Company Entry Descriptions – PAYROLL and PURCHASE
June 19, 2026	▪ Fraud Monitoring by (all other) [non-consumer] Originators, TPSP, and TPS ▪ ACH Credit Monitoring by (all other) RDFIs

Best Business Practices in Fraud Management

Guidance Examples

- Access and approval systems: Establish multiple levels of approval and implement multifactor authentication to verify identities for authorized staff dealing with cash disbursements and other transactions that require approval to help reduce the risk of fraud. Multiple levels of approval can also slow the process and provide greater opportunity to identify suspicious attributes or markers for certain transactions.
- Verification of documents: Implement verification processes for documents originating from third parties to combat the risk of AI-generated fraudulent documentation. For example, organizations can establish direct communication channels with issuers of critical documents rather than merely accepting provided documents at face value.

Guidance Examples

- Collaboration and information sharing: Establish a team or committee (e.g., operations, internal audit, risk management, IT, cybersecurity, and professionals from other functions) to monitor relevant advances in AI technology and regularly update risk assessments, security protocols, and fraud detection systems geared to emerging capabilities.
- Training and communication: Improve and provide continuous training so you can increase employee awareness of new and evolving types of fraud while also reinforcing appropriate courses of action to remedy any breaches.

Guidance Examples

- Financial institutions should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.
- The rule does not require monitoring to be performed prior to processing Entries.
- For transactions in which monitoring identifies as suspect, the ODFI can consider a number of actions. Actions may include, but are not limited to, stopping further processing of a flagged transaction; consulting with the Originator to determine the validity of the transaction; consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags, or requesting the freeze or the return of funds.

Guidance Examples

- An RDFI might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk.
- An entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Guidance Examples

- These risk-based processes and procedures do not require the screening of every ACH Entry individually, and they do not need be performed prior to processing Entries.
- The requirement to establish processes and procedures reasonably intended to identify Entries suspected of being unauthorized or authorized under False Pretenses should not be interpreted to impose an obligation on RDFIs to prevent wrongful activity.

Guidance Examples

While a RDFI will not likely know the circumstances under which a credit Entry was originated, Entries that are unauthorized or authorized under False Pretenses potentially may be identified based on characteristics of the Entry and the receiving account, such as:

- A Standard Entry Class Code that does not align with the type of receiving account, such as a corporate CCD entry to a consumer account.
- A high-dollar transaction that is unusual for the receiving account.
- A series of similar credit Entries received within a short period of time, such as multiple payroll or benefit payments.
- Any of the above to a new account, a dormant account, or to an account acting as a money mule.

Advanced Fraud Detection Technologies

Combating Generative AI Fraud

- Combating generative AI fraud requires a multifaceted approach, leveraging machine learning for real-time detection, promoting human oversight, maintaining legal and ethical standards, and fostering cross-industry collaboration.
- Real-time fraud detection and prevention are bolstered by machine learning's ability to:
  - Analyze transactions as they happen
  - Safeguard assets
  - Secure customer trust
  - Protect the FI's reputation

Machine Learning Fraud Detection

- Diverse machine learning methods are employed in fraud detection, which include but are not limited to:
  - Anomaly detection
  - Risk scoring
  - Network analysis
  - Behavioral biometrics
- These methods help identify unusual patterns, evaluate the likelihood of fraud, uncover networks of fraud, and examine customer transaction patterns and behaviors.

Human Oversight and Verification

- Despite the crucial role of AI in fraud detection, the necessity of human oversight cannot be overstated.
- Oversight helps mitigate false positives, improve customer experience, and ensure fairness and accountability in fraud control.
- Financial institutions should invest in continuous training for their teams to recognize signs of fraudulent activities, complementing AI detection systems and contributing to overall security.

Legal and Regulatory Requirements

- Addressing data privacy, AI liability, and intellectual property concerns within the context of generative AI fraud necessitates robust legal and ethical frameworks.
- Compliance with regulations like the Nacha Rules, GLBA, and UDAAP is necessary to safeguard data privacy.

Resources

Resources

- Guidance and Information Involving Payments
  - https://www.nacha.org/content/regulatory-guidance
- Training, Membership and Consulting Information
  - https://simplifyrisk.stout.com/
- Fraud Risk Management Guide COSO and ACFE
  - https://www.acfe.com/-/media/files/acfe/pdfs/fraud-risk-tools/coso-fraud-risk-management-guide-second-edition-executive-summary.pdf

Questions

STOUT

Presenter

Kelly Rozier, AAP APRP

Associate

krozier@stout.com

Office: +1.404.369.1143