Fraudster's Toolbox: ACH Fraud

Presented By: Joy Babcock, AAP, AFPP

Disclaimer

- PaymentsFirst, through its Direct Membership in Nacha, is a specially recognized and licensed provider of ACH education, publications and support.
- Payments Associations are directly engaged in the Nacha rulemaking process and Accredited ACH Professional (AAP) program.
- Nacha owns the copyright for the Nacha Operating Rules & Guidelines.
- The Accredited ACH Professional (AAP) and Accredited Payments Risk Professional (APRP) is a service mark of Nacha.
- This material is derived from collaborative work product developed by Nacha and its member Payments Associations and is not intended to provide any warranties or legal advice and is intended for educational purposes only.
- This material is not intended to provide any warranties or legal advice and is intended for educational purposes only.
- This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.
- No part of this material may be used without the prior written permission of PaymentsFirst.
-

Agenda

- Common ACH Fraud Schemes
- Emerging Fraud Technologies
- Detecting and Mitigating Risk
- Case Studies

What is ACH Fraud?

ACH fraud is a form of cybercrime involving unauthorized transactions through the ACH network, allowing criminals to steal directly from bank accounts using stolen routing and account numbers. It often includes phishing, business email compromise, or fake invoices to illicitly transfer funds, with high risks to businesses and individuals.

Why Target ACH?

- High volume and speed
- Limited real-time verification
- Reliance on account/routing numbers

Meet the Fraudster

- Organized and opportunistic
- Tech-savvy and adaptive
- Exploits human and system weaknesses

The Fraudster's Toolbox

- Social Engineering
- Stolen Credentials
- Malware
- Account Manipulation
- Timing Strategies

Social Engineering

- Phishing emails
- Impersonation (vendors, executives)
- Urgent payment requests
- Red Flags
  - Urgent tone
  - Unusual payment changes
  - Slight email/domain differences

Stolen Credentials

- Online banking login theft
- Credential stuffing
- Weak password exploitation
- Account Takeover Red Flags
  - Login from new location/device
  - Sudden changes in behavior
  - Password resets followed by transactions

Malware

- Keyloggers
- Banking trojans
- Remote access tools
- Red Flags
  - Unusual system activity
  - Multiple failed logins
  - Transactions initiated without user awareness

Business Email Compromise (BEC)

- Fraudster poses as trusted party
- Requests ACH payment changes
- Targets accounts payable staff
- Red Flags
  - Vendor banking detail changes
  - Requests outside normal process
  - Pressure to bypass controls

Insider Threats

- Employees misusing access
- Data theft or manipulation
- Red Flags
  - Access outside job role
  - Unusual transaction patterns
  - After-hours activity

Timing Attacks

- Initiating transactions before weekends/holidays
- Exploiting cutoff times
- Red Flags
  - Late-day transactions
  - Activity before non-processing days

Emerging Fraud Trends

AI Synthetic Identity Fraud

- Combines real information with fabricated data to create synthetic identities
- Personas are used to open new accounts
- Creates legitimate-looking credit histories
- Used for large scale ACH fraud

False Pretenses and Authorized Push Payments

- False Pretenses
  - Fraudsters use BEC to convince businesses to “voluntarily” send payments
  - Vendor or Payroll impersonation
- Authorized Push Payment Fraud (APP Fraud)
  - Tricking victims into willingly authorizing a real-time bank transfer to a fraudulent account

Ghost Funding

- Fraudsters exploit the time lag in ACH transfers to gain immediate access to funds that have not yet settled
- Initiate a transfer from an empty account to an investment or trading app
- Uses the instant credit to purchase assets and withdraw funds, leaving the FI with the loss

Detecting and Mitigating Risk

Behavioral Analytics

- Establish a baseline of normal customer and business behavior
- Flag anomalies like:
  - First-time ACH originations
  - Sudden increase in dollar amounts or volume
  - Changes in payee patterns
- Use risk scoring to prioritize alerts for review

Transaction Monitoring

- Monitor ACH files and individual entries in real time or near real time
- Key triggers to watch:
  - New payees or changes to existing payees
  - Out-of-pattern SEC codes
  - Transactions just under approval thresholds
- Implement velocity controls
- New Fraud Monitoring Rules 2026

Dual Control and Segregation of Duties

- Require at least two individuals to initiate and approve ACH transactions
- Separate roles for setup, approval, and release of payments
- Regular staff training and audits

Logins and Monitoring

- Detect logins from unusual geolocations or devices
- Identify impossible travel scenarios
- Monitor repeated failed login attempts followed by success
- Utilize Multi-Factor Authentication (MFA)
- Payment Verification Processes

Alerting and Escalation

- Set tiered alerts (low, medium, high risk)
- Ensure clear escalation paths for frontline staff
- Train staff on what to do when alerts trigger

Toolbox Defenses

- MFA
- Account Alerts
- Real-Time Monitoring
- Fraud Alerts
- Audit Logs
- Activity Tracking

Case Studies

Account Takeover

Janice has a small embroidery business and logs into online banking from her usual device. Unbeknownst to her, she accessed an unsecure website earlier that day and malware was downloaded onto her device that captured her credentials. Later that evening, a fraudster logs in from a different state, adds a new payee, and initiates a $45,000 ACH credit.

- What happened?
- What are the Red Flags?

Business Email Compromise

Willow Record Store receives an email that appears to be from their marketing vendor that is well known to them. They regularly receive ACH payments from the record store. The email states:

“Hi! We’ve recently updated our banking information. Please send all future payments to the attached account effective immediately.”

The branding, signature, and tone all look legitimate. The accounts payable clerk updates the ACH instructions and sends a $65,000 payment.

Two days later, the real vendor calls asking where their payment is.

- What is the red flag?
- What could have prevented the loss?

The Inside Job

Rob works in accounting and has access to initiate ACH payments. Over four months he:

- Creates a “vendor” that is actually his personal account
- Sends weekly ACH credits of $750
- Labels them as “misc operational expenses”

No one noticed because the amounts are small, consistent, and reporting only covers large transactions.

- Why is this type of fraud so hard to detect?
- What control would have made this much harder to execute?

Questions?

AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

AFPP
Accredited Faster
Payments Professional™

PaymentsFirst

Continuing Education Credits

Fraudster's Toolbox: ACH Fraud

May 27, 2026

This session is worth 1.2 credits. Please keep this slide for your records.

Contact Us

(678)-384-9791

www.paymentsfirst.org

education@paymentsfirst.org

@PaymentsFirst