Bluefin®

Navigating Nacha: Rules, Policies, and Compliance Strategies for Higher Education

2025

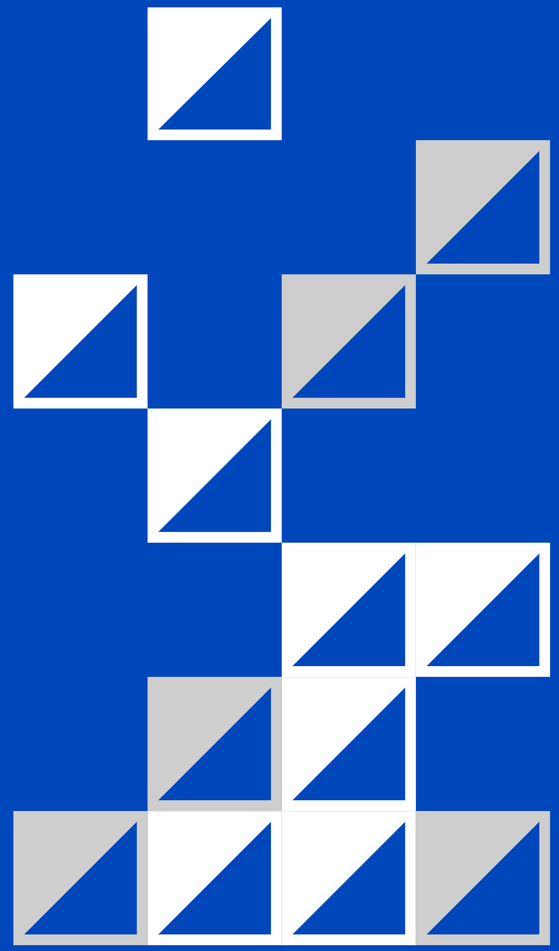
Welcome & Agenda

Housekeeping

- Webinar duration / Questions / Recording

Today’s Agenda

- Nacha overview and why it matters for higher education
- Operating Rules, cybersecurity implications, and campus use cases for ACH
- Key Nacha Rule amendments coming into effect in 2025-2026
- Best practices, tools, and resources to help your institution stay secure and compliant



Your Presenters

Ruth A. Harpool, AAP, APRP, CTP
CampusGuard Treasury Solutions Advisor,
Nacha ACH Network Advisory Board Member

Ruston Miles
Founder & Chief Strategy Officer
Bluefin

What is Nacha?

- Nacha (originally the National Automated Clearing House Association) is a nonprofit that governs the U.S. ACH (Automated Clearing House) Network

- The ACH Network enables electronic money transfers, including direct deposits, electronic bill payments, and recurring debits

Helpful Tip
Learn more abut ACH:
https://achdevguide.nacha.org/how-ach-works

Key Functions

Rules & Standards
Writes and updates the Operating Rules & Guidelines.

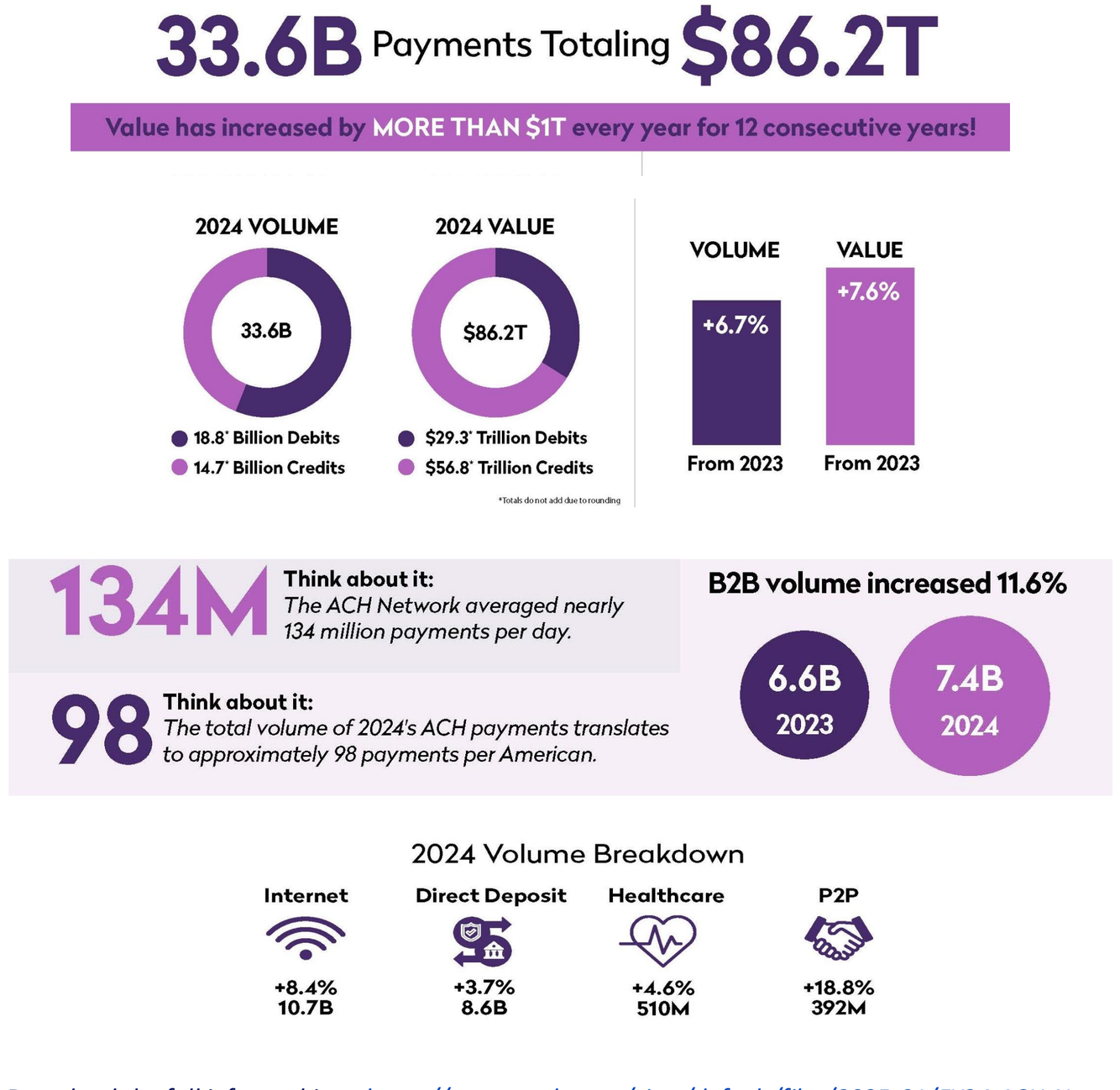
Guidance & Oversight
Ensures compliance and arbitrates violations

Education & Innovation
Provides training, certifications (AAP, APRP), and risk/fraud resources.

Risk Management
Operates monitoring programs and databases for compliance.

Nacha®

ACH volume is increasing due to businesses moving away from checks, the growing adoption of faster payment methods like Same Day ACH, and increased usage in areas like B2B and P2P payments.



** Download the full infographic at https://www.nacha.org/sites/default/files/2025-01/FY24-ACH-Network-Infographic.pdf*

Operating Rules & Guidelines

Provides the legal, operational, and risk framework for all ACH participants

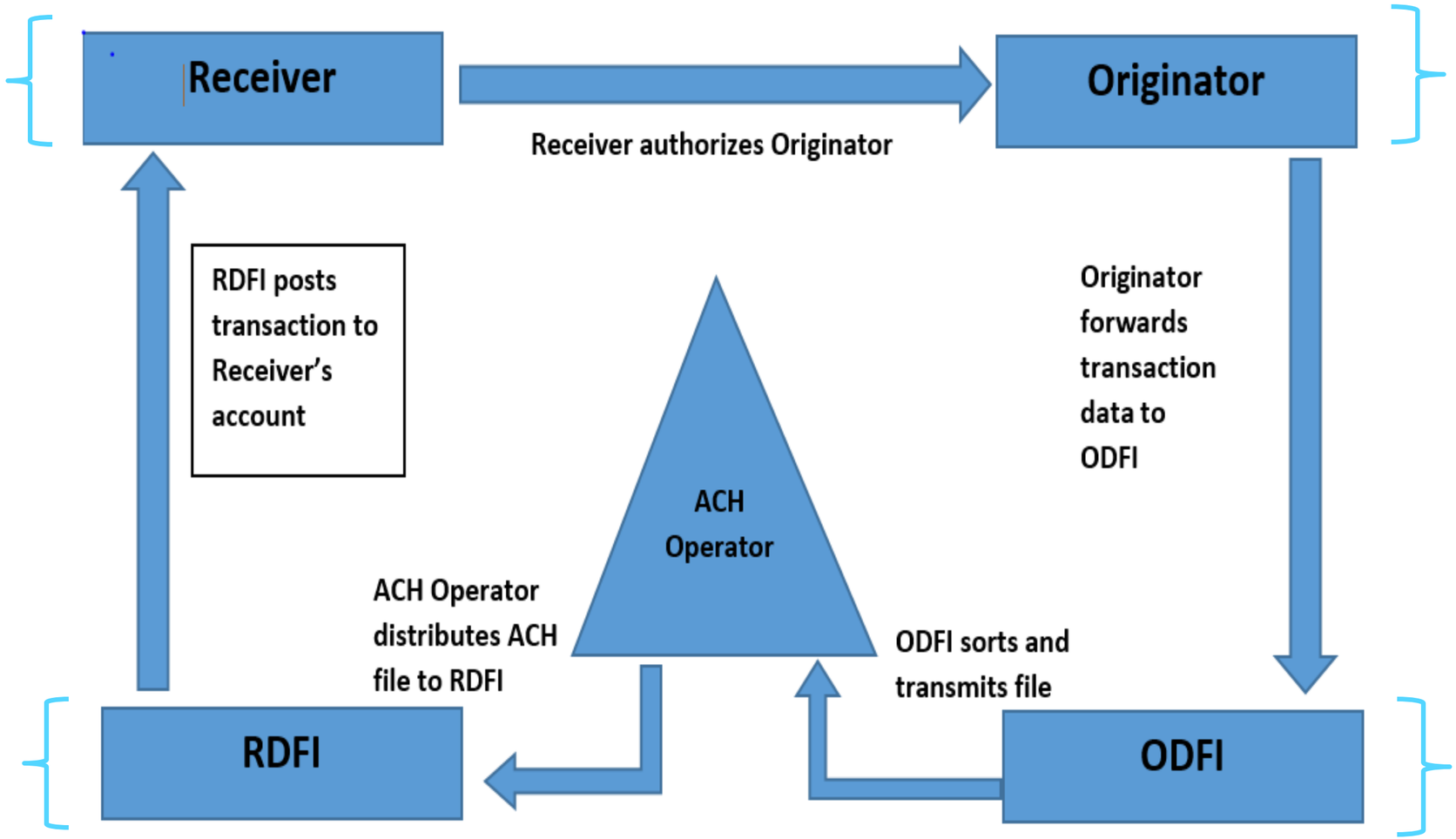
ACH Participant	Role / Responsibility Highlights
Originator	The party (often a business) that initiates ACH entries (credits or debits) through an ODFI. Must comply with originator requirements, warranties, proper authorization, etc.
ODFI (Originating Depository Financial Institution)	The bank or financial institution that accepts entries from originators and forwards them into the ACH Network. Must adhere to risk controls, proper formatting, return handling, etc.
RDFI (Receiving Depository Financial Institution)	The institution that receives ACH entries for its account holders (receivers). It has obligations like posting, return windows, responding to return requests, etc.
Third-Party Sender / Third-Party Service Provider (TPSP / TPP)	Entities acting as intermediaries between originators and ODFIs; they are subject to additional oversight, responsibility, and contractual obligations.
ACH Operator(s)	The central clearing entities (e.g. Federal Reserve, The Clearing House) that route, settle, and perform exchange of ACH entries, following rules around files, timing, etc.

√ The Rules define the legal and regulatory obligations of participants.	**√ The Guidelines expand upon the Rules with commentary, examples, best practices, and operational detail.**	**√ The Rules & Guidelines are updated (generally annually) along with supplements.**

Tuition Bill Payment – Example

ACH Debit

Student or Parent paying tuition



University

Student or Parent's bank

University's Bank

Nacha and Cybersecurity

There is a cybersecurity risk each time that financial information is moved and stored

For Higher Ed:

- $3.7M average breach cost
- 70% increase in ransomware attacks
- 4,388 cyberattack attempts per week*

ACH compliance isn't just about moving money - it's about protecting sensitive data

Advantages of ACH Under Nacha

Safe Payments
Protects sensitive data.

Smart Payments
Rules evolve with technology.

Fast Payments
Supports quicker processing.

Fraud Reduction
Safeguards against financial crime.

Secure Data
Prevents theft, misuse or disclosure.

Avoid Penalties
Non-compliance fines can reach $500,000/month.

Compliance
Strengthens institutional reputation.

** IBM Cost of a Data Breach report, 2023 report; Malwarebytes 2023 report; CheckPoint, Q2 2025 report*

The Importance of ACH for Colleges and Universities

Payroll & employee disbursements (direct deposit).

Student refunds / financial aid disbursements.

Tuition & fee payments (one-time and recurring debits).

Third-party processor compliance.

Fraud risks & monitoring (refund fraud, phishing).

Reconciliation, returns, disputes.

Compliance audits & risk management.

ACH Across the Higher Ed Environment

ACH Rule Amendments Overview

1

Fraud Monitoring Rule

2

Standard Company Entry Description Rule

3

Data Security Requirements

ACH Fraud Monitoring Rule

The ACH Fraud Monitoring Rule is part of Nacha's broader Risk Management initiative to combat credit-push fraud. **Credit-Push fraud** is where funds are pushed from a payer's account to a fraudster's account (e.g., via payroll scams, vendor impersonation, or business email compromise)

The Rule **requires** ACH Originators, Third-Party Service Providers(TPSP), Third-Party Senders (TPSs) and ODFIs with 6 million+ to implement **risk-based fraud monitoring processes** reasonably designed to detect fraudulent ACH credit entries.

Effective Dates:

- March 20, 2026 — Applies to Originators, Third Party Service Providers (TPSP), and ODFIs with 6M+ transactions annually.
- June 22, 2026 — Extends to **all** other Originators and Receiving Depository Financial Institutions (RDFIs)

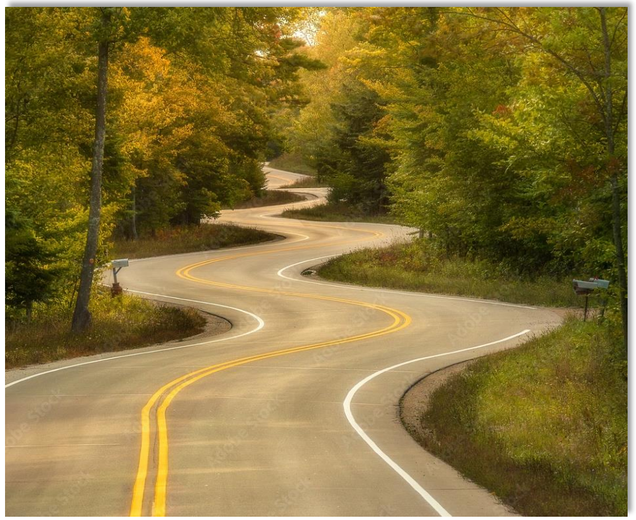
Why Adopt the Fraud Monitoring Rule Now?

Higher Education face **risks** from:

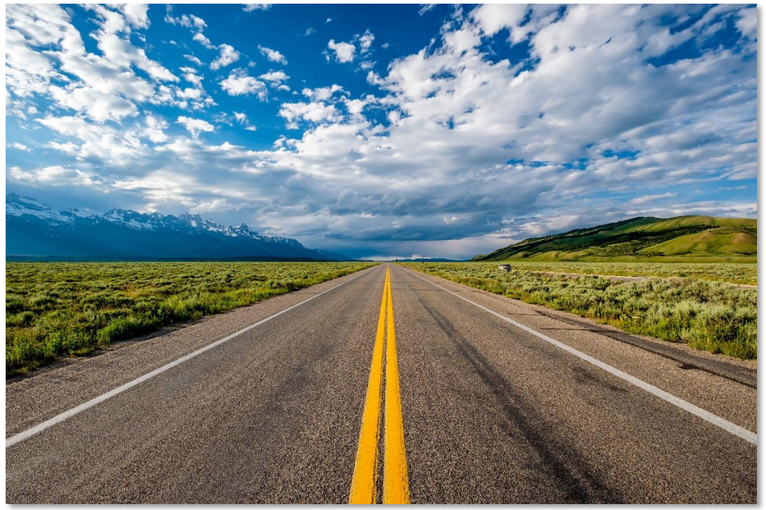
- Payroll Fraud
- Student refund scams
- Vendor impersonation attacks

Benefits of adopting the Rule:

- Proactive Risk Management
- Improved Fund Recovery
- Reputation Protection
- Alignment with Best Practices
- Support for Internal Audits and Compliance



Versus



From Understanding to Execution

ACH Fraud Monitoring Rule

Things to know:

- Requires that institutions implement documented, risk-based processes to detect fraudulent ACH entries. Monitoring should include velocity checks, anomaly detection, and behavioral tolerances.
- Monitoring is continuous, not one time
- Special attention required for Micro-Entries used in account verification

Things to do:

- Create and/or maintain written ACH and fraud policies
- Conduct ACH risk assessments
- Conduct regular audits, training, and policy and procedure reviews to ensure ongoing compliance
- Use secure data storage, verify new receivers, and scrutinize account changes.
- Collaborate with trusted partners like Bluefin and CampusGuard for compliance support

Supplementing Data Security Requirements Rule

The Supplementing Data Security Requirements Rule mandates that certain ACH participants must render deposit account information unreadable when stored electronically.

This Rule **requires** compliance from Originators, TPSPs, and TPSs with ACH volume exceeding 2 million transactions annually.

Once the 2 million mark is surpassed the requirement remains in effect, regardless of whether your next annual transaction volume hits the threshold or not.

Effective Dates:

- June 30, 2021, if originating over 6 million transactions annually
- June 30, 2022, if originating over 2 million transactions annually

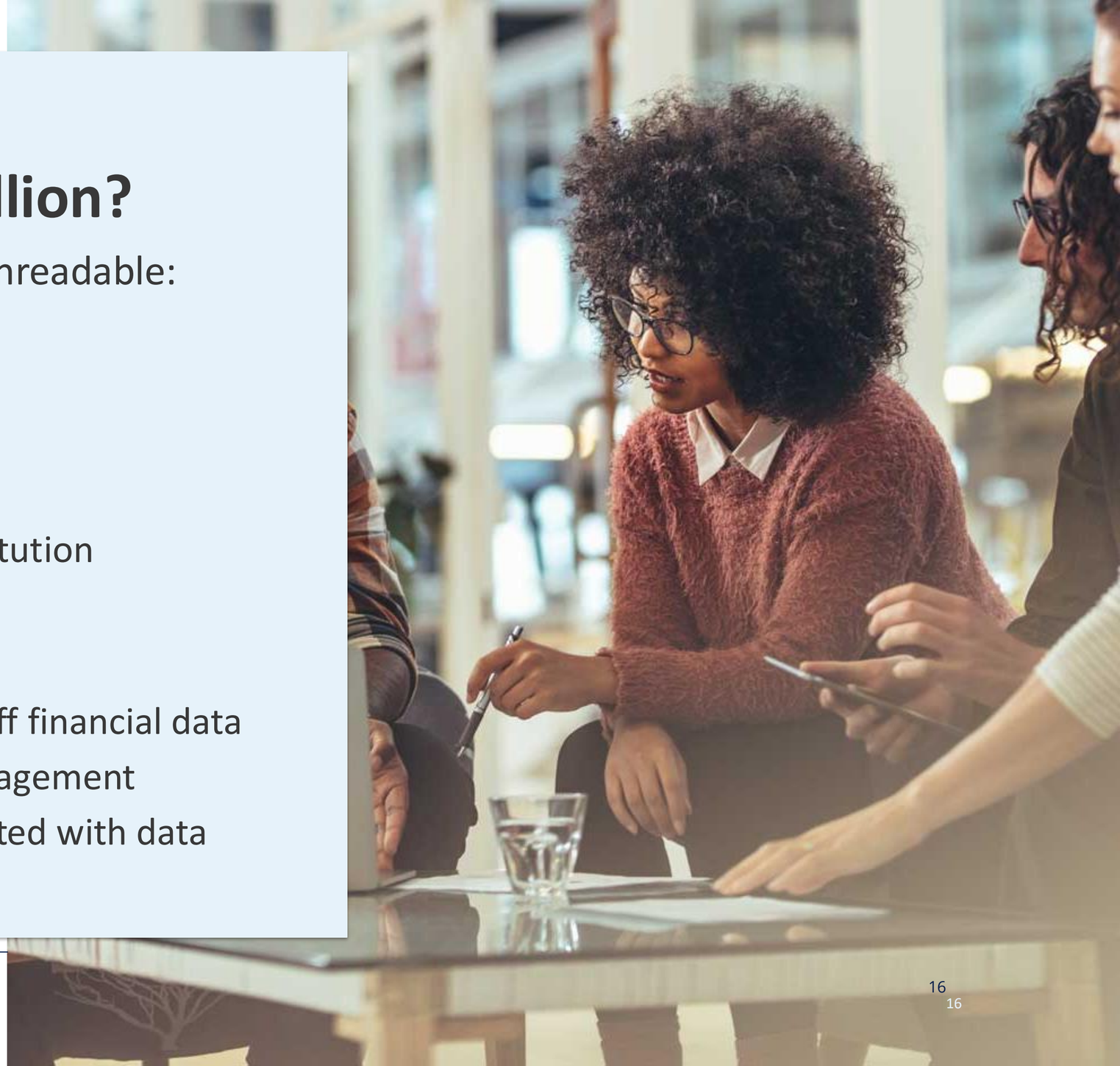
Why Adopt the Rule if Originating Under 2 Million?

Acceptable methods of rendering unreadable:

- Encryption
- Tokenization
- Truncation
- Destruction
- Secure hosting by a financial institution

Benefits of adopting the Rule:

- Protects student, donors, and staff financial data
- Demonstrates proactive risk management
- Reduces reputational risk associated with data exposure incidents.



16

From Understanding to Execution

Supplementing Data Security Requirements Rule

Things to know:

- Data (deposit account information) must be rendered unreadable when stored electronically.
- Security is a Shared Responsibility
  - ODFIs must identify and notify clients who are newly covered by the rule.
  - Higher Education institutions must coordinate with their banks and vendors to ensure compliance.

Things to do:

- Institutions must maintain written ACH policies that define:
  - Roles and responsibilities for ACH origination
  - Data protection standards
  - Retention and breach reporting procedures
- Regular assessments, audits, and training are recommended to ensure ongoing compliance.
- Seek support from trusted partners, be that and ODFI,

Standard Company Entry Description Rule

The Standard Entry Description Rule is part of Nacha's broader Risk Management initiative aimed at reducing fraud and improving transaction transparency across the ACH Network.

It requires ACH Originators to use standardized language in the "Company Entry Description" filed of ACH transactions to clearly identify the purpose of the payment.

Effective March 20, 2026:

- Requires "PURCHASE" in all caps for e-commerce transactions.
- Requires "PAYROLL" for payroll transactions.

Likely easy to implement, but reliance on FI partners may slow adoption.

Why It Matters for Higher Education

- Clarifies the payment purpose for RDFI’s will improve fraud detection and funds availability logic.
- Supports monitoring tools that rely on consistent transaction labeling to flag anomalies.
- Standardize e-commerce purchases using the term “PURCHASE” for WEB debit entries authorized online.

From Understanding to Execution

Standard Company Entry Description Rule

Things to know:

- PAYROLL descriptor for PPD Credits
  - The Company Entry Description field must contain “PAYROLL” for PPD credits used to pay wages, salaries, or similar compensation.
- PURCHASE descriptor must be used for WEB debit entries authorized by consumers for online purchase of goods.
- THIS DOES NOT APPLY TO SERVICES OR CCD credits in B2B transactions.

Things to do:

- PURCHASE should not be used for vendor payments or CCD credits
- PAYROLL may include Contractors expecting payroll-like treatment

How The Rules Shape ACH Risk Management in Higher Education

Nacha's direction = stronger operational discipline

The three new rules signal a shift from "set-and-forget" compliance to *active, continuous risk governance.*

Not just for high-volume institutions

Even if thresholds (2M+ or 6M+ entries) don't apply yet, the expectations define best practices for *everyone handling ACH data or payments*.

Higher Ed implications

Universities face a mix of decentralized finance operations and legacy systems, making early adoption a *strategic differentiator* and risk reducer.

Best Practices

Data Security: Encrypt or tokenize stored ACH files *now* – don't wait for the 2M threshold. Ensure backups and shared drives meet "unreadable data" standards.

Fraud Monitoring: Use ACH transaction monitoring tools or dashboards to flag anomalies (e.g., duplicate refunds, out-of-pattern disbursements). Connect this to BEC prevention programs.

Standardization: Review internal and third-party Nacha file templates. Align field descriptions and codes ("PAYROLL", "PURCHASE") across systems to avoid failed entries.

Testing and documentation: Implement annual testing. Treat compliance like a "seatbelt" that only works if regularly checked. Create a living document of processes and audit trails.

CampusGuard and Bluefin

Compliance and security for colleges & universities

Assess
Powered by CampusGuard

- Conducts comprehensive Nacha/ACH risk assessments to identify policy and control gaps.
- Evaluates third-party and processor compliance with institutional and Nacha standards.
- Reviews cybersecurity maturity across policies, systems, and incident response.
- Provides ongoing reassessments to track changes and emerging risks.

Secure
Powered by ShieldConex®

- Tokenizes sensitive data at capture.
- Format-preserving tokens drop directly into legacy and modern applications with no workflow disruption.
- Secures high-risk fields including student ID, SSN, bank account, and payment details at the source.
- Extends protection to admissions, student health centers, and financial services.

Store
Powered by FileGuard

- Secures ACH, financial aid, and donor batch files through encryption and tokenization.
- Protects sensitive data during SFTP and other file-based transfers: no exposure in transit.
- Integrates seamlessly with legacy and cloud platforms such as Ellucian, Workday, and Oracle.
- Ideal for institutions using FTP workflows or scheduled exports, ensuring end to end data protection.

Next Steps / Resources

Next Webinar - Securing the Future: Protecting Higher Education from Data Breaches

The Payments Academy
November 12th, 3 – 4 pm EST
https://www.thepmtsacademy.org/

Ruston Miles
Founder & Chief Strategy Officer
Bluefin

Terry Ford
SVP Strategic Partnerships
Bluefin

Resources / Downloads

- Important Updates to the ACH Fraud Monitoring Rule
- ACH Assessment Benefits Guide
- CampusGuard Nacha/ACH Services
- Bluefin for Higher Education
- Bluefin ShieldConex / FileGuard

Q&A / Thank You!

Ruth A. Harpool, AAP, APRP, CTP
CampusGuard Treasury Solutions
Advisor, Nacha ACH Network Advisory Board Member

Ruston Miles
Founder & Chief Strategy Officer
Bluefin