Somehow, I Manage to Control My Risk: Instant Payments

Jessica Lelii, AAP, AFPP, APRP, NCP

Director of Education

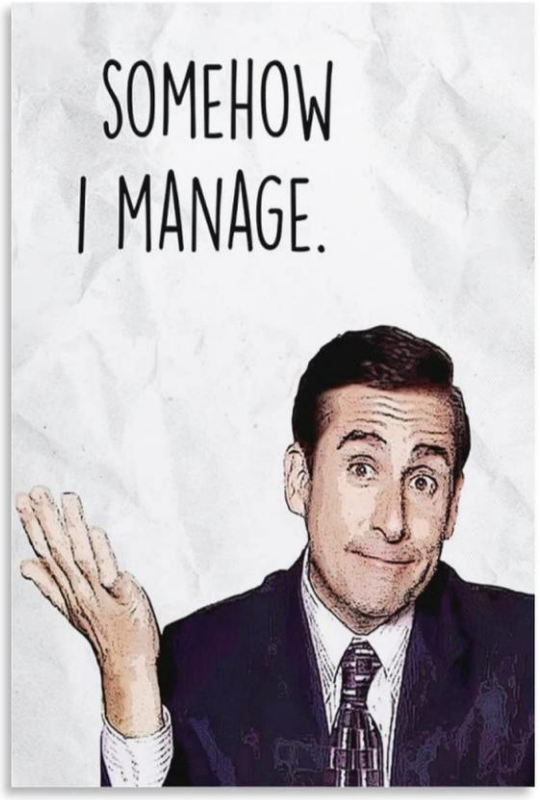
PaymentsFirst

jlelii@paymentsfirst.org

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



- Instant Payments Overview
- Risk Assessment
- Fraud Risk
- Other Risk Mitigation
  - Operational Risk
  - Cross-Channel Risk
  - Third-Party Risk

Instant Payments Overview

Instant Payments

- credit push only
- use real time gross settlement
- enable both payer and payee to see the transaction reflected in their respective account balances immediately
- offer immediate funds availability to the payee
- final and irrevocable

FedNow Characteristics

Created and operated by the Federal Reserve

Allows financial institutions to send credits on a 24x7x365 basis with instant clearing, settlement, and posting

Utilizes the FedLine electronic communication system to connect financial institutions to the Federal Reserve's payment and information infrastructure

Current network transaction value limit is $10,000,000

- The default limit for financial institutions is $100,000; however, this limit may be lowered by the FI for individual customers

RTP Characteristics

Real Time Payments (RTP) is a product created and operated by The Clearing House (TCH)

Allows participating financial institutions to send credits on a 24x7x365 basis with instant clearing, settlement, and posting

Financial institutions may connect directly to the service, or they may utilize a third-party processor

- Non-bank payment service providers connect via a participating financial institution

Current network transaction value limit is $10,000,000

Stages of an Instant Payment

1. Initiation: the sending FI authenticates the sender and receives a payment instruction from the sender via a supported channel.

2. Validation: Sending FI, FedNow/RTP, and Receiving FI complete their validation steps.

3. Response: The receiver FI reviews the message and responds with either:
   - Accept
   - Accept without post
   - Reject

4. Settlement: FedNow/RTP will affect settlement to both the Sending and Receiving FIs.

5. Posting and Notification: The Receiving FI will provide funds availability to the Receiver's account and both the Sender and Receiver are notified.

Risk Assessment

Somehow, I Manage to Identify and Assess my Risk

Risk Assessment: Measures the effectiveness of the control activities to determine the level of residual risk remaining

- Residual risk – the portion of risk remaining after mitigation measures have been applied

Mapping the risks to each control helps the organization find any gaps remaining in its compliance program

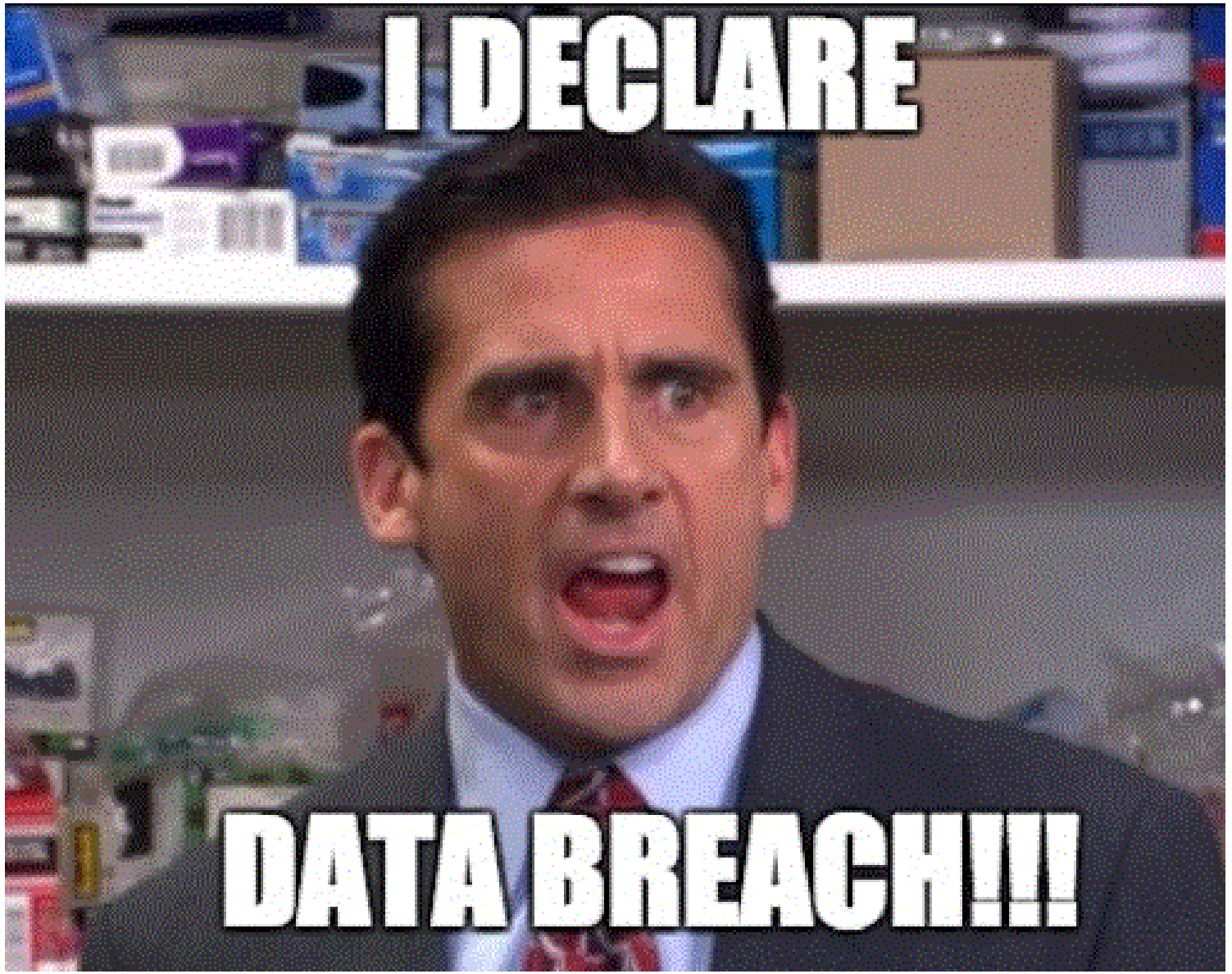
Risk assessment should:

- Estimate the significance of the risk
- Assess the likelihood or frequency of the risk occurring
- Consider how the risk should be managed and assess what action must be taken

Risk Assessment

Overall process of risk identification, analysis, control, and evaluation

- Risk Identification – Finding, recognizing, and describing risks
  - Can involve historical data, theoretical analysis, informed, and educated opinions, and shareholders' needs
- Risk Analysis – Process to comprehend nature of and determine level of risks
  - Foundation for risk evaluation
  - Includes risk estimation
- Risk Controls – Process implemented to control identified risk
- Risk Evaluation – Process of comparing risk analysis results to determine if controls are effective and residual risk is acceptable



Somehow, I Control my Fraud Risk

Fraud Terms

Fraud: an act of deception, misrepresentation, or dishonesty intended to result in financial or personal gain, or to cause a loss to another party.

False Pretenses: the inducement of a payment by a Person misrepresenting (a) that Person's identity, (b) that Person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited. (Article Eight, Section 8.42)

Scam: a deceptive scheme designed to trick someone out of their money or personal information.

Financial Exploitation: the illegal or improper use of an individual's money, property, or other resources for personal gain. It often involves deception, coercion, or undue influence to obtain assets without the individual's consent.

Pig Butchering: a sophisticated investment scam that involves building a long-term, trusting relationship with the victim, often through romance scams, before tricking them into investing in fake cryptocurrency or other fraudulent schemes.

Types of Fraud that Use Instant Payments

Authorized Push Payments

Impersonation scams

- Payroll scams

“Phantom Hacker” scams

Romance scams

Investment scams

Account Takeover

Credential harvesting

Mule account layering

Business-Specific Scams

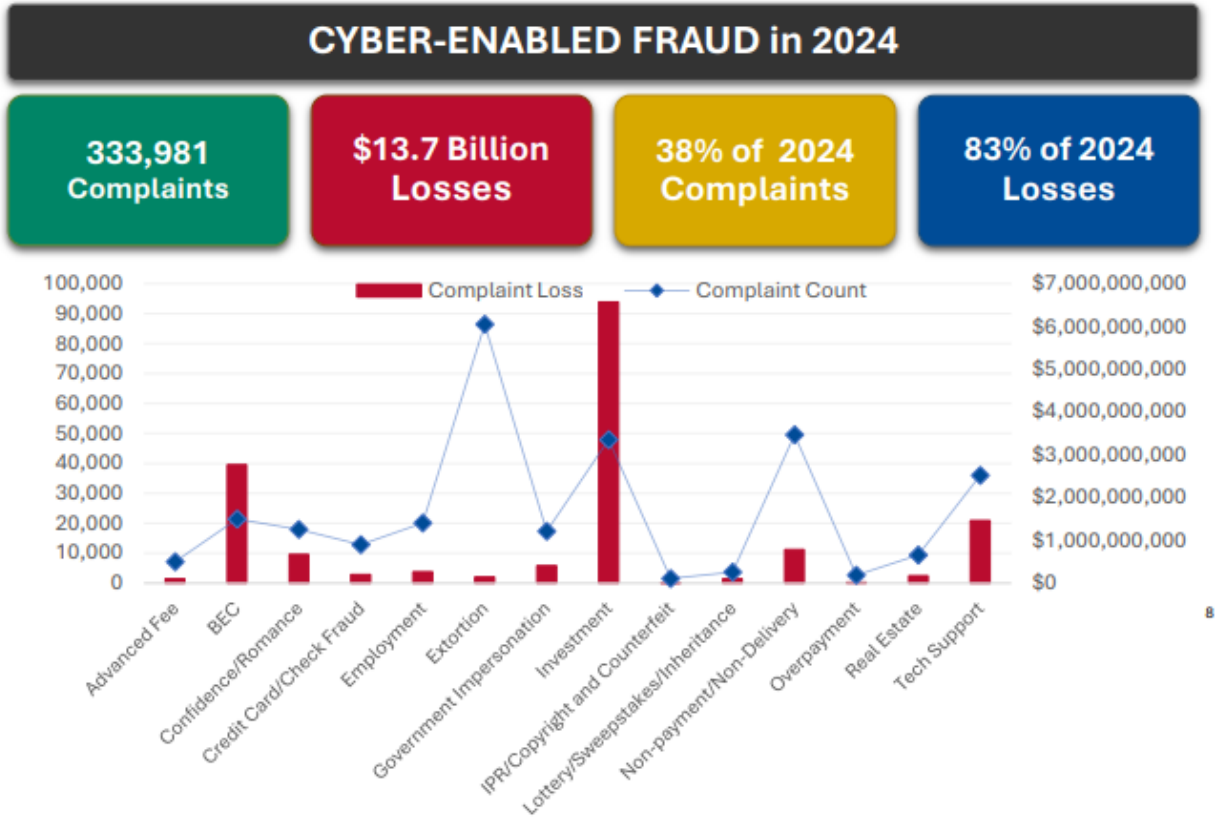
Business email compromise

- Invoice Redirection
- Executive Impersonation
- Vendor Impersonation

CYBER-ENABLED FRAUD

Cyber-enabled fraud includes complaints where criminals use the Internet or other technology to commit fraudulent activities, often involving the theft of money, data, or identity, or the creation of counterfeit goods or services. Cyber-enabled fraud is responsible for almost 83% of all losses reported to IC3 in 2024.

7



8

2024 IC3 Annual Report

Top Ways Funds Are Lost in Fraud

- Cryptocurrency
- Wire transfer/ACH
- Debit/Credit Card
- Peer-to-Peer Transfer
- Gift/Prepaid Card
- Check/Cashier's Check
- Cash

2024 IC3 Annual Report

What is a Control?

A process designed to provide assurance regarding the achievement of objectives relating to operations, reporting and compliance

Policies, procedures or other safeguards put into place to reduce the amount of risk posed to your institution

Controls reduce risk and help ensure management’s directives to mitigate risk

Combatting Fraud

Think in terms of layers of safeguards

- In addition to internal systems and processes, educating customer and leveraging security measures built into the payment network are important complements.

Review fraud solutions and processes

- Identify opportunities for improvement, particularly for those based on batch processing and manual intervention.

Talk with vendors and technology partners

- Discuss new approaches, including applying real-time fraud-detection capabilities and achieving a comprehensive view of transaction patters across all payment types.

Add suspicious accounts and aliases to a watch list

- This will block potentially fraudulent transactions before funds leave your institution.

Stay involved and informed

- Join industry councils or conferences to keep appraised of developments in the fraud landscape and share insights with peers.

Somehow, I Control my Fraud Risk

- Anti-malware software (a.k.a. anti-virus, anti-spyware)
  - Provides a defense against keyloggers and man-in-the-middle (MIM)/man-in-the-browser (MIB) attacks
  - Used to prevent, detect, block and remove adware, spyware and other forms of malware

- Transaction monitoring/anomaly detection software
  - Monitors online banking activity for suspicious funds transfers
  - Detect and stop a suspicious ACH/wire transfer before completion and alert institution

- Out-of-band authentication
  - Transaction initiated via one delivery channel (e.g., Internet) must be reauthenticated or verified via an independent delivery channel (e.g., telephone) in order to complete the transaction

Somehow, I Control my Fraud Risk

Internet protocol (IP) address authentication or static IP requirement

Individual and aggregate exposure limits

Negative lists

Dual control

KYC and KYCC

Ongoing training of frontline and operations staff

CIP training

Security training

Business Continuity training

Somehow, I Control my Fraud Risk

Multi-Factor Authentication uses a combination of two or more authentication factors

Multi-Factor Authentication considered ‘commercially reasonable” for verifying identity in electronic access

Three Authentication Factors:

- Something the user knows
  - Password, PIN
- Something the user has
  - Token, mobile device
- Something the user is
  - Biometric characteristic

Authentication Method Types

Biometric

- Physical features unique to an individual
- More secure than knowledge-based verification

Device binding

- Links user's identity to a specific device

Risk-based

- Analyzes multiple factors to determine the level of necessary security
- Compares factors against known behavior
- Based on perceived risk
- Requires additional steps for high-risk transactions

Commercially Reasonable Security

According to UCC Article 4A, to determine what is commercially reasonable, you should consider:

- Size of financial institution
- Type of customer
- Type of payment order
  - Frequency of transactions
  - Nature of business
- Similarly-situated customers doing similarly related activity

Commercially reasonable methods and techniques used to detect fraud

Trend analysis

Machine learning

Predictive and behavioral modeling

Anomalous transaction detection

Enhanced due diligence

Confirmation of payee

Fraud Detection and Mitigation

Approach	Methods and techniques	Type of fraud	
		Authorized	Unauthorized
Technology	Confirmation-of-Payee (CoP)	X	
	Fraud monitoring system/trend analysis and anomaly detection	X	X
	Biometric and behavioral authentication	X	X
	Digital ID		X
	Fraud negative lists (fraudulent individual database)	X	X
Regulation and scheme rules	Transaction value and volume limits	X	X
	Transaction hold for analysis	X	X
	Strong customer authentication/ multi-factor authentication	X	X
	Fraud reporting transparency (e.g., industry-wide reporting with clear, standardized, and transparent fraud classifications)	X	X

Other Risk Mitigation

Somehow, I Control my Operational Risk

Audit programs

Policies and procedures

Business continuity management

IT support – maintenance and system upgrades

- Address “downtime” based on instant payment channel

Reconciliation

Dual Control

Staff Training

- Accredited Staff – AFPP or APRP

Agreements

Somehow, I Control my Cross-Channel Risk

An enterprise-wide view of retail payments risk

- Understanding how each payments system interrelates

Effective internal controls including financial, accounting, technical, procedural and administrative

Good funds model for payment initiation

- Value/velocity/volume limits

Anomalous detection software

Layered security

- Dependent on nature of payment system

Audit programs

Somehow, I Control my Third-Party Risk

Vendor/TPSP Policy

Vendor Management Program

- Due diligence
- Ongoing monitoring
- Business Continuity Management

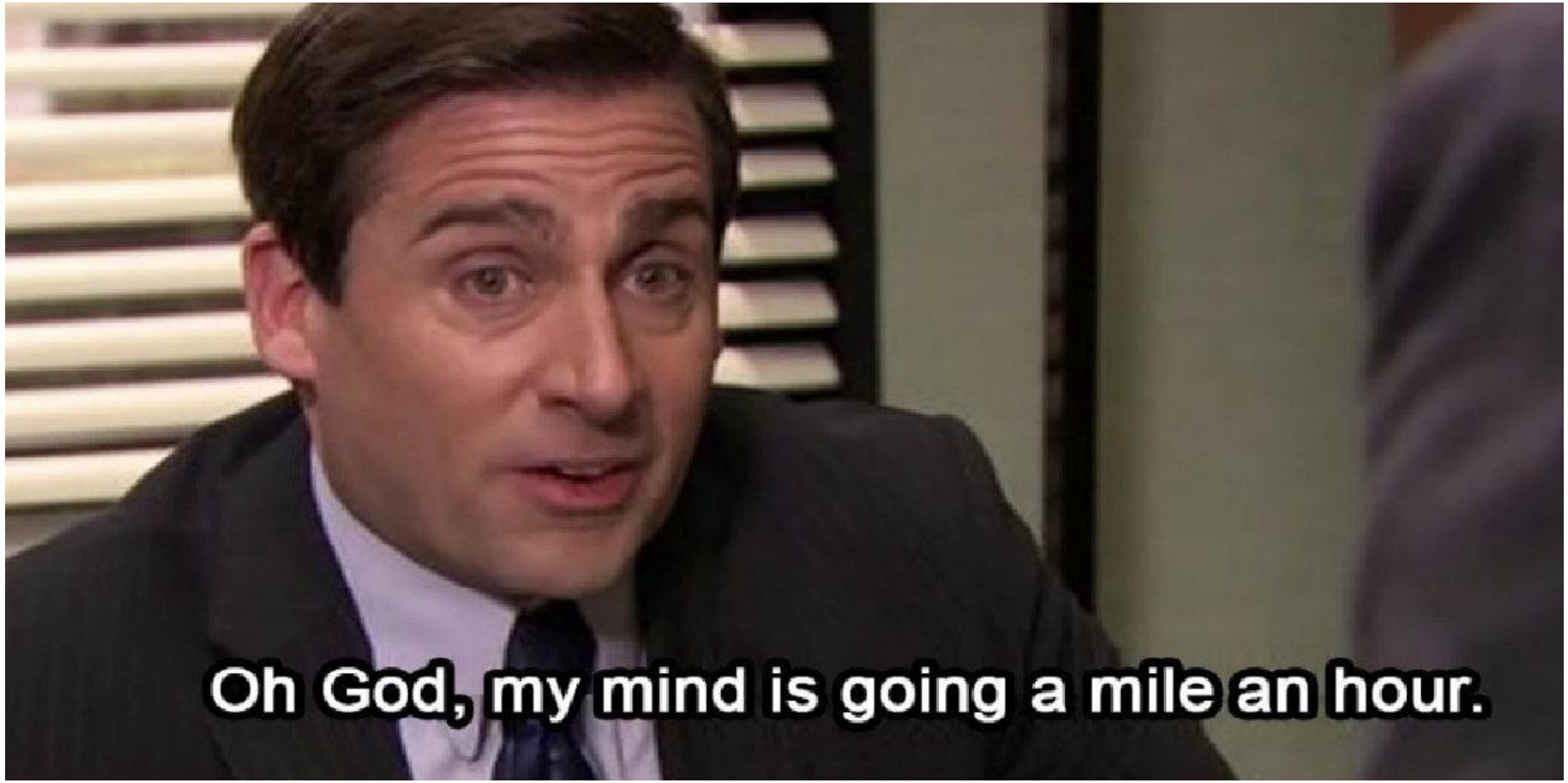
Third-Party agreements

Audit

Risk Assessment

Continuing Education/Training

QUESTIONS?



AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

AFPP™
Accredited Faster
Payments Professional

PaymentsFirst

Continuing Education Credits

Somehow, I Manage to Control my Risk – Instant Payments

February 2026

This session is worth 1.2 credits

(keep this slide for your records)

Contact Us

(678)-384-9791

www.paymentsfirst.org

education@paymentsfirst.org

@PaymentsFirst