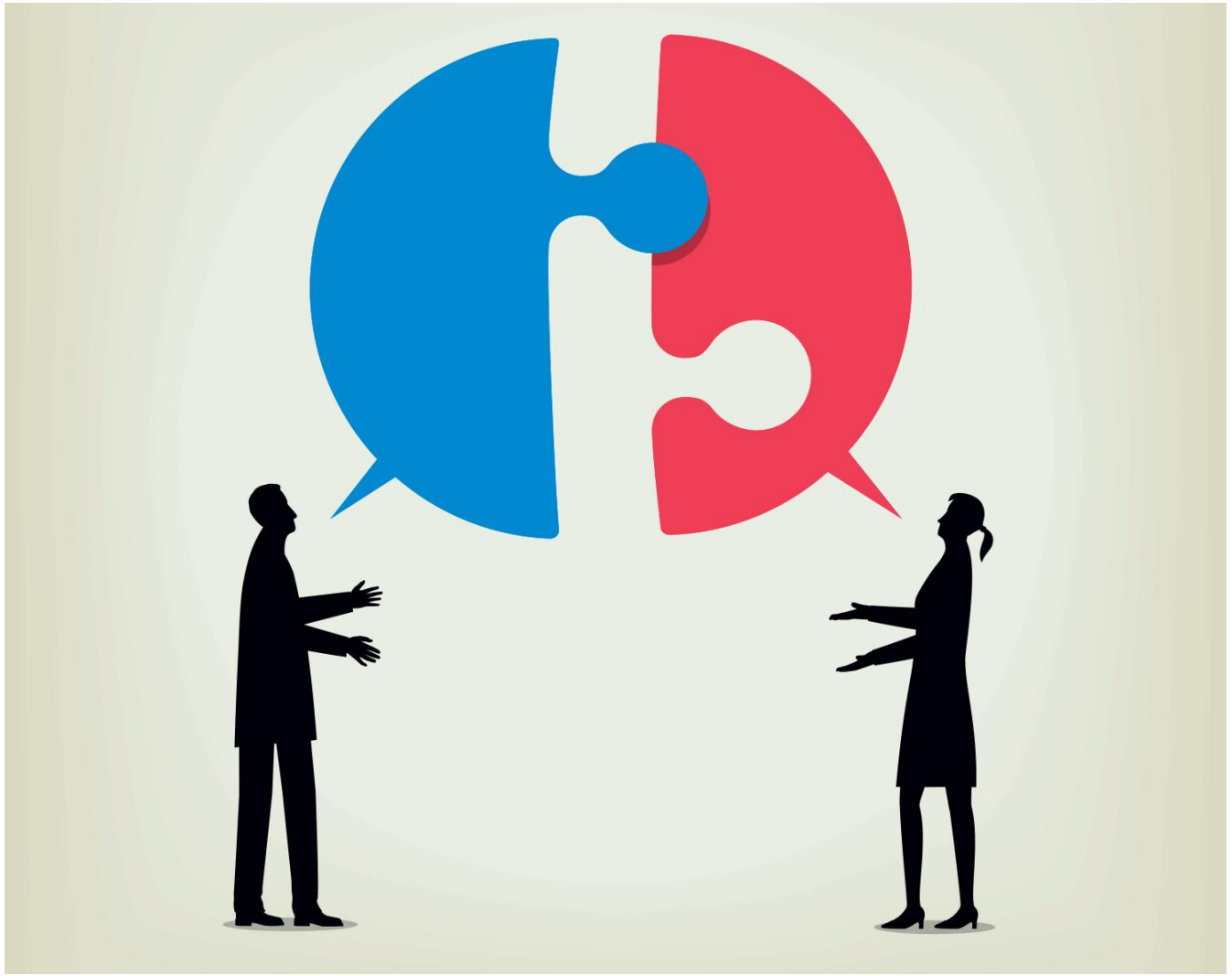


Logical Friction in Electronic Payments

Controlling Error and Fraud in Electronic Payments

JESSICA LELII, AAP, APRP, NCP
DIRECTOR OF EDUCATION
PAYMENTSFIRST
JLELII@PAYMENTSFIRST.ORG

DISCLAIMER

Macha, 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 Macha/PAR.

Risk Management

Risk vs. Reward

Risk: All payment systems have inherent risk

Reward: Ability to offer a variety of services to your account holders

Risk Appetite and Tolerance

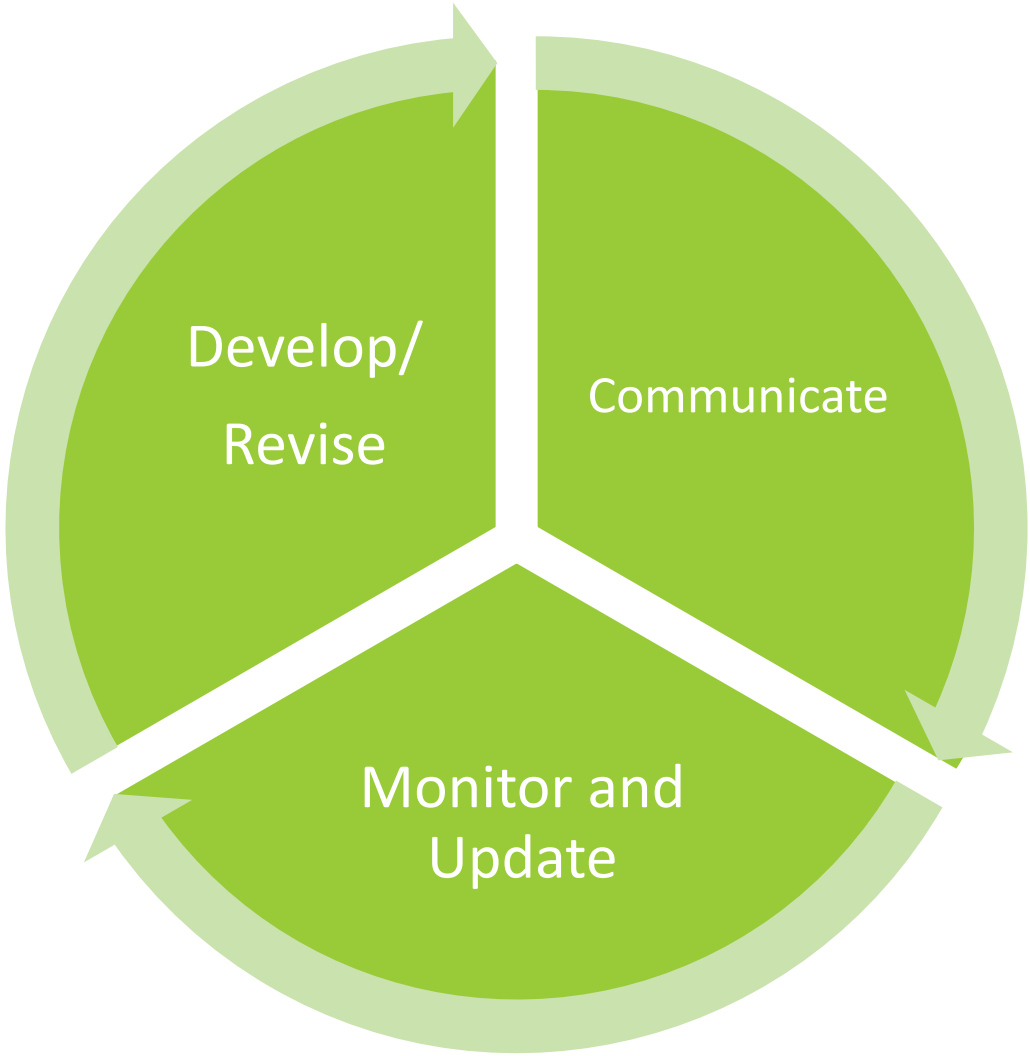
Risk Appetite: the amount of risk, on a broad level, an entity is willing to accept in pursuit of value

- Reflects the entity's risk management philosophy
- Influences the entity's culture and operating style
- Guides resource allocation

Risk Tolerance: the acceptable level of variation relative to achievement of a specific objective

- Operating within your risk tolerance helps ensure that the entity remains within its risk appetite

3 Steps to Determine Risk Appetite



Risk Profile

Description of any set of risks

- Can apply to entire organization, department, or particular category

Organizational Risk Profile encompasses all internal risk profiles

- Snapshot of organization's risk appetite

Vary significantly

- Size and complexity of financial institution's retail products/services, IT infrastructure, and use of third-parties

Risk Profile

An FI's risk profile is affected by many factors:

- Size of the FI
- Complexity of the payments systems it offers
- Frequency and dollar amounts of payments
- Types of payments initiated
- Payment delivery methods
- IT infrastructure
- Dependence on third parties/vendors
- Emergence of new payment instruments
- Protection of non-public personal information

Risk Management

Identify	Risk Assessment
Measure	Risk Analysis or Evaluation
Mitigate	Implement controls
Monitor	Tracking and reporting

Friction in Payments

What is friction in payments?

Lengthy forms

Multiple steps and redirects

Confusing or unclear navigation

Frustration or inconvenience

Processing delays

Inconsistent experiences

Lack of Trust and Security

Friction in Payments – Why is it so challenging?

Damaged brand reputation: A poor payment experience can tarnish a brand's reputation and lead to negative reviews.

Increased accountholder effort: As a result of hurdles, accountholders must spend more time and effort to complete their transactions, leading to frustration and dissatisfaction.

Inconvenient, leading to frustration

Complex passwords can be difficult to remember and manage

Fraud

The FTC reported consumers lost over $12.5 billion to fraud in 2024.

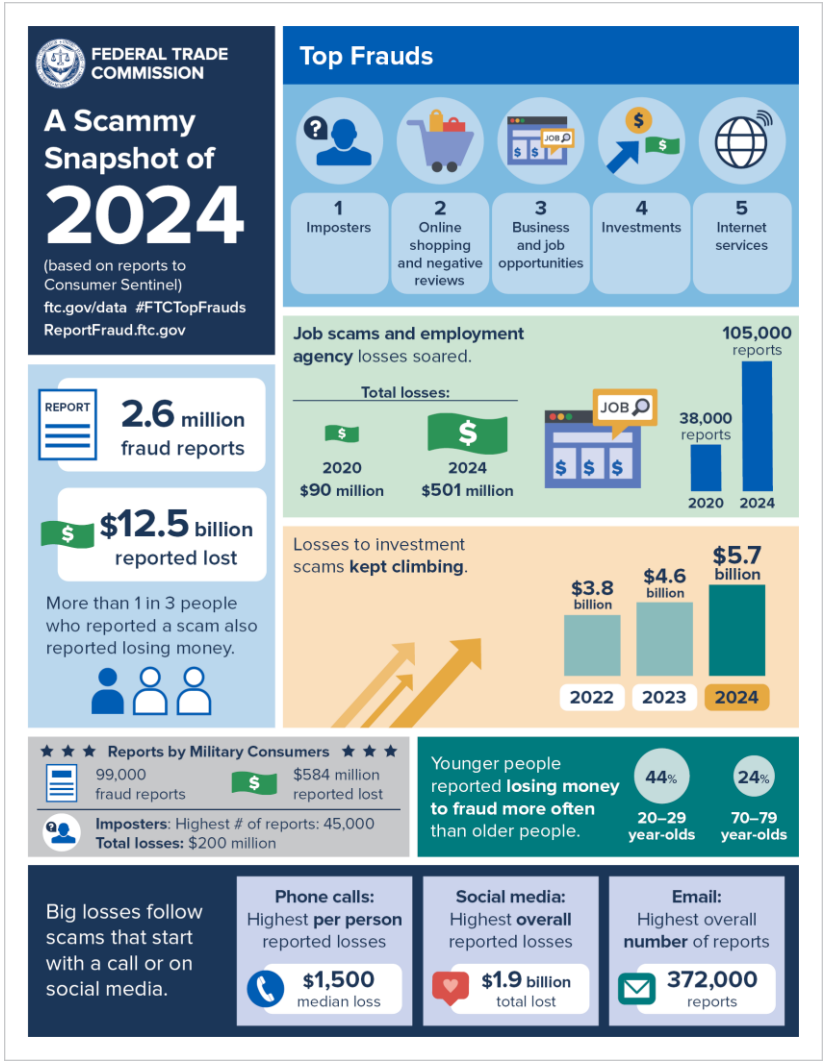
- This was a 25% increase from the previous year.
- These losses resulted from scams and account takeover fraud.
  - Investment Scams were the highest category of reported loss - $5.7 billion
  - Imposter Scams were the second highest category of reported loss - $2.95 billion

The most significant business losses have resulted from:

- Account takeover
- Data breaches
- Phishing attacks
- Business email compromise

Growing reliance on online platforms for transactions and communication has created more opportunities for cybercriminals.

Many individuals and businesses are not sufficiently aware of the latest threats and how to protect themselves.



Financial Institution Loss

Financial institutions may have obligations to recredit accountholders without a guarantee of recovery

- Regulation E
- UCC 4A
- Nacha Operating Rules
- Other private sector rules (RTP, FedNow, Zelle, etc)
- Account and Service Agreements
- Vendor agreements

Logical Friction

What is logical friction?

The balancing act between security and convenience

A point of logical friction creates a hurdle, block, or pausing point for an end-user accessing payment services, allowing a reasonable opportunity to exercise extra caution

Helping your accountholders help themselves!

Cannot approach as a burden or pain point

Opportunity to strengthen relationships and build trust

Authentication and Verification

Multi-factor Authentication (MFA)

- Requiring users to verify their identity through multiple methods

Biometric Authentication

- Using biometric data like fingerprints, facial recognition, or voice recognition

Device Verification

- Verifying the device used for logins

Geolocation Verification

- Confirming the user’s location

Account Validation

- Verifying the validity of account information, prior to a live transaction

Risk-Based Authentication

Adaptive Authentication

- Adjusting the level of authentication based on risk factors, such as:
  - Transaction amount
  - Location
  - Device

Step-up Authentication

- Requiring additional verification steps for high-risk transactions can reduce the likelihood of fraud

Transaction Monitoring and Alerts

Real-time Transaction Monitoring

- Continuously monitoring transactions for unusual patterns or high-risk activities

Fraud Alerts

- Sending alerts to accountholders for suspicious activity, prompting them to take action

Card Controls

- Allowing cardholders to set spending limits, block specific merchants, or enable card controls based on location

Advanced Fraud Detection Technologies

Machine Learning and AI

- Utilizing advanced algorithms to analyze large datasets and identify patterns of fraudulent behavior can improve detection accuracy

Behavioral Biometrics

- Monitoring user behavior, such as typing speed and mouse movements, can help identify anomalies and potential fraud

Education and Awareness

Security tips and Best practices

- Providing information on how to protect accounts, recognize phishing attempts, and avoid common scams

Phishing Awareness training

- Educating accountholders about the tactics used by phishers

Collaboration with law enforcement

Regular Security Updates

- Keeping accountholders informed about the latest security threats and how the financial institution is addressing
  - Helps to build trust and confidence

Logical Friction in Action

Online Account Opening - Risks

Identity theft

Synthetic identity fraud

Money mule accounts

Accounts used in scams

Loan fraud

Violating USA Patriot Act

Collecting inaccurate information

Account funding transactions

Controlling Online Account Opening Risks

KYC and Due Diligence

Information and Document Verification

Suspicious Activity Monitoring

Behavioral Biometrics

Machine Learning

Multi-factor Authentication (MFA)

Secure Communication Channels

Layered Security

Call backs or thank you cards

Mailing all initial documents to physical address associated with TIN/SSN

Establish prerequisites to electronic services

Value, volume and velocity limits

Access

Due diligence/KYC

Multi-factor authentication

Strong password policies

Regular updates to applications

Multi-Factor Authentication

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

Controls by Payment Channel

ACH

Transaction alerts/push notifications
- Affirmative responses

Value and velocity limits

Real time monitoring

Delaying funds availability
- In compliance with Regulation CC

CARD

Transaction monitoring

Activity alerts/notifications
- Affirmative responses

Dynamic value and velocity limits

Controls by Payment Channel

CHECK AND RDC

Risk-based item review

Signature comparisons
- Establish thresholds

Deposit limits and controls
- Value and velocity
- Types of checks

Extended holds
- Establish thresholds within Regulation CC compliance

WIRE TRANSFER

Value and velocity limits

Out of band verifications/challenges
- Callbacks

Transmittal or confirmation forms

Dual control

You Decide!

What services do you want to offer?

Who is allowed to use the service?

Internal Controls

Who?

Things you should consider:

- Account relationship
- Tenure of relationship
  - New account holder?
- History of account activity
  - Account balances
  - NSFs
  - Regulation E Claims
  - Recurring Deposits

Educate!

Be Proactive, Not Reactive!

- Know current fraud trends and scams.
- Provide education/information to your staff and account holders
  - Social Media
  - Flyers/Brochures
  - Videos
  - Emails
  - Newsletter

Moral of the story

- Be selective
- Implement strong controls
- Review, Revise, Repeat
- Educate!

AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

Continuing Education Credits

Logical Friction

April 2025

This session is worth 1.8 credits

(keep this slide for your records)