

March 28, 2025

# PERSPECTIVE



**CHANGES EVERYTHING.**

**WIPFLI**

## About the presenters

**Krista A. Moran, CERP**

Manager, Risk Advisory Services

krista.moran@wipfli.com

203.518.8315

[wipfli.com](http://wipfli.com)

**Andrew Morgenroth, AAP, CMQCS**

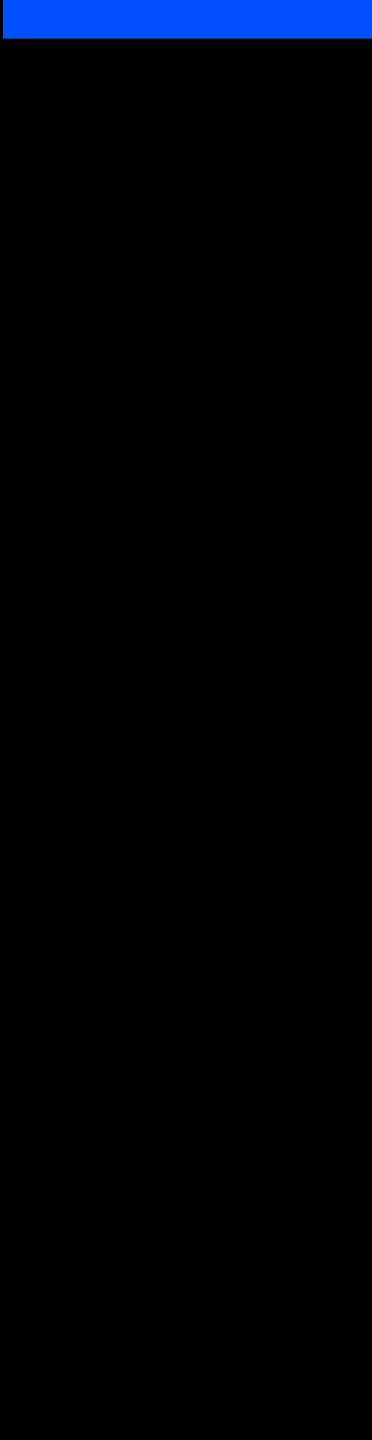
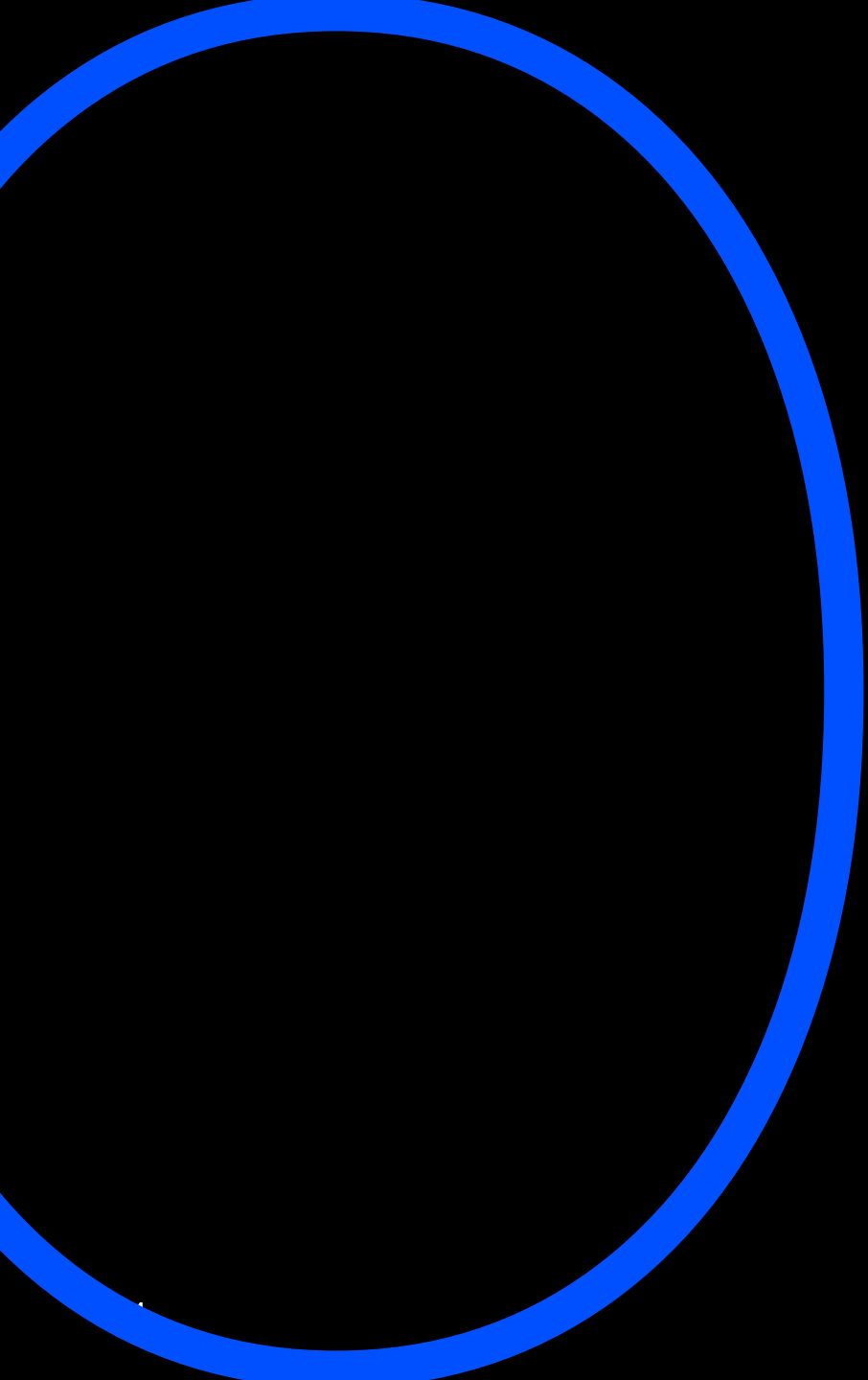
Manager, Risk Advisory Services

amorgenroth@wipfli.com

815.484.5686

## Overview

Wire Transfers	04
Risk Mitigation	11
Key Controls	15
Common Findings	19
Nacha rule changes	21
Fraud prevention	35
ACH - Originators	38
About Wipfli	56

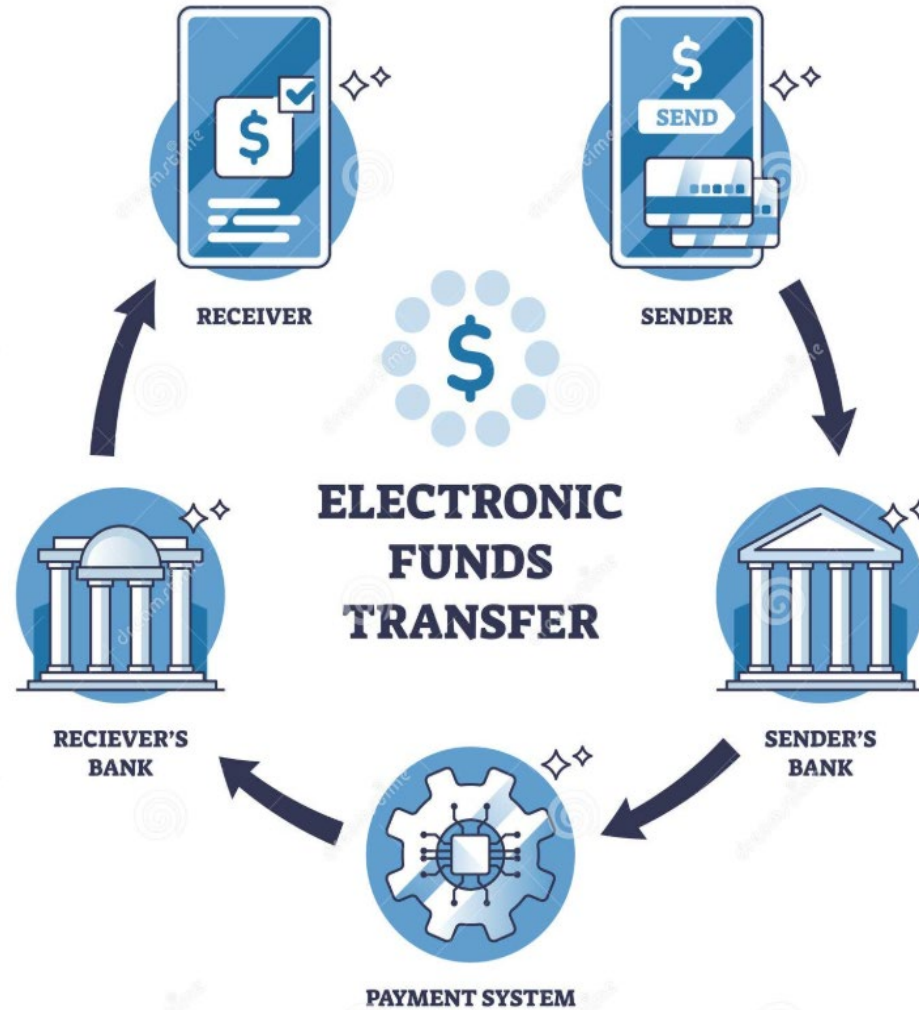


Wire Transfers

# Overview

Wire Transfers are a method of electronic funds transfers from one person or entity to another for both domestic and international transactions

# Wire Transfer Life Cycle



# POLL 1

*Risk assessments are crucial for identifying and mitigating potential risk.*

## Risk Assessments!

### Operational Risk

- The risk of loss resulting from inadequate or failed internal processes, people and systems, or external events that result in an inability to deliver products, remain competitive, and manage information

### Strategic Risk

- Strategic risk is the risk of adverse business decisions through management's actions or inactions

### Compliance Risk

- Current & prospective risk to earnings arising from violations of, or nonconformance with, laws, rules, regulations, internal policies and procedures, or ethical standards

### Reputation Risk

- Reputation risk is the risk of negative public opinion or perception leading to a loss of confidence and/or severance of relationships

### Fraud Risk

- Employees and other insiders
- External sources – An individual could obtain a member's identity and make a fraudulent request to transfer to an outside source.

### Credit Risk

- The risk that the receiver or originator of a transaction does not have sufficient funds to settle the transaction

**Don't forget to add a review date and to review periodically (at least annually)**



*Risk assessments are crucial for identifying and mitigating potential risk.*

## Risk Assessments!

### Liquidity Risk

- Current & potential risk to earnings or capital arising from a CU's inability to meet its obligations when they come due without incurring unacceptable losses
- A CU does not have enough funds to cover outgoing electronic transfers, and
- A CU transfers funds out before those funds have been received

### Third Party Risk

Credit unions that use a third party (for example, a corporate credit union or CUSO) to process electronic payments are subject to third-party risk. Retail, payroll, and wire transfer companies (for example, Western Union, MoneyGram, and PayPal) are other third parties that introduce risk.

<https://publishedguides.nca.gov/examiner/Content/ExaminersGuide/ElectronicPaymentSystems/ExamProcedures/WireTransfer1-Prelim.htm>

## Key Risk Indicators

### Key Risk Indicators

#### Compliance – lack of compliance with:

- Bank Secrecy Act
- Dodd-Frank
- Inadequate or ineffective agreements/contracts

#### Credit

- Weak controls regarding source & availability of funds
- Weak controls over exception handling
- Inadequate controls over:
  - Dollar limits, activity thresholds, & Transaction types

#### Liquidity

- Ineffective controls over daylight overdrafts, dollar limits and activity thresholds
- Inadequate Risk Assessments over high-risk customers or activities

## Key Risk Indicators

### Key Risk Indicators

#### Operational Risk

- Inadequate Risk Management program
- Insufficient Policy and Procedures
- Inadequate Management Oversight or Documentation
- Inadequate Internal Controls
- Inadequate Training
- Inadequate Incident Response Plan and/or Business Continuity Plan
- Lack of or Inadequate Third-Party Risk Program

#### Reputational Risk

- Untimely postings, downtime, and lack of system and software reliability

#### Strategic Risk

- Lack of Board Awareness and/or Risk Appetite
- Lack of Strategic Planning or Growth without a project plan
- New services or use of a third-party without Adequate Due Diligence



Risk Mitigation

# Risk Mitigation

## Board Oversight

- A credit union's board of directors should establish the objectives, risk tolerances, and policies including:
  - Effective Internal & External Audit
  - Priority on Information security
  - Business Continuity Planning
  - Vendor Management

## Management

- A credit union's management team is responsible for carrying out the board - established business plan

## Procedures

- Timely Posting, Balancing and Reconciliation of accounts
- Clear CIP procedures
- Enhanced Due Diligence on high - risk activity
- Provisions for dual controls and separation of duties
- User threshold limits
- Exception Handling

## Risk Mitigation

### Segregation of Duties & Dual Control

Maintaining appropriate dual control and segregation of duties over wire processes is important to ensure no single person has control over the entire process end -to -end.

Every wire system should be set up to require at least two separate participants in a wire transfer:

- The person who inputs or requests the transfer
- The person who verifies and sends the transfer

When a credit union uses the Federal Reserve systems, the EUAC is responsible for assuring the credit union's wire transfer system and procedures require dual control. Ideally, the EUAC should not have processing capabilities.

Smaller credit unions may not have individual departments devoted to these functions and may have staff members perform more than one function related to transfers. In these cases, the credit union should have sufficient management oversight and controls in place to ensure adequate segregation of duties.



## Key Employee Roles

Board

Management

Member Services

Accounting

IT Department

Wire Department



Key Controls





# Internal Control

*[in-'tər-nəl kən-'trō]*

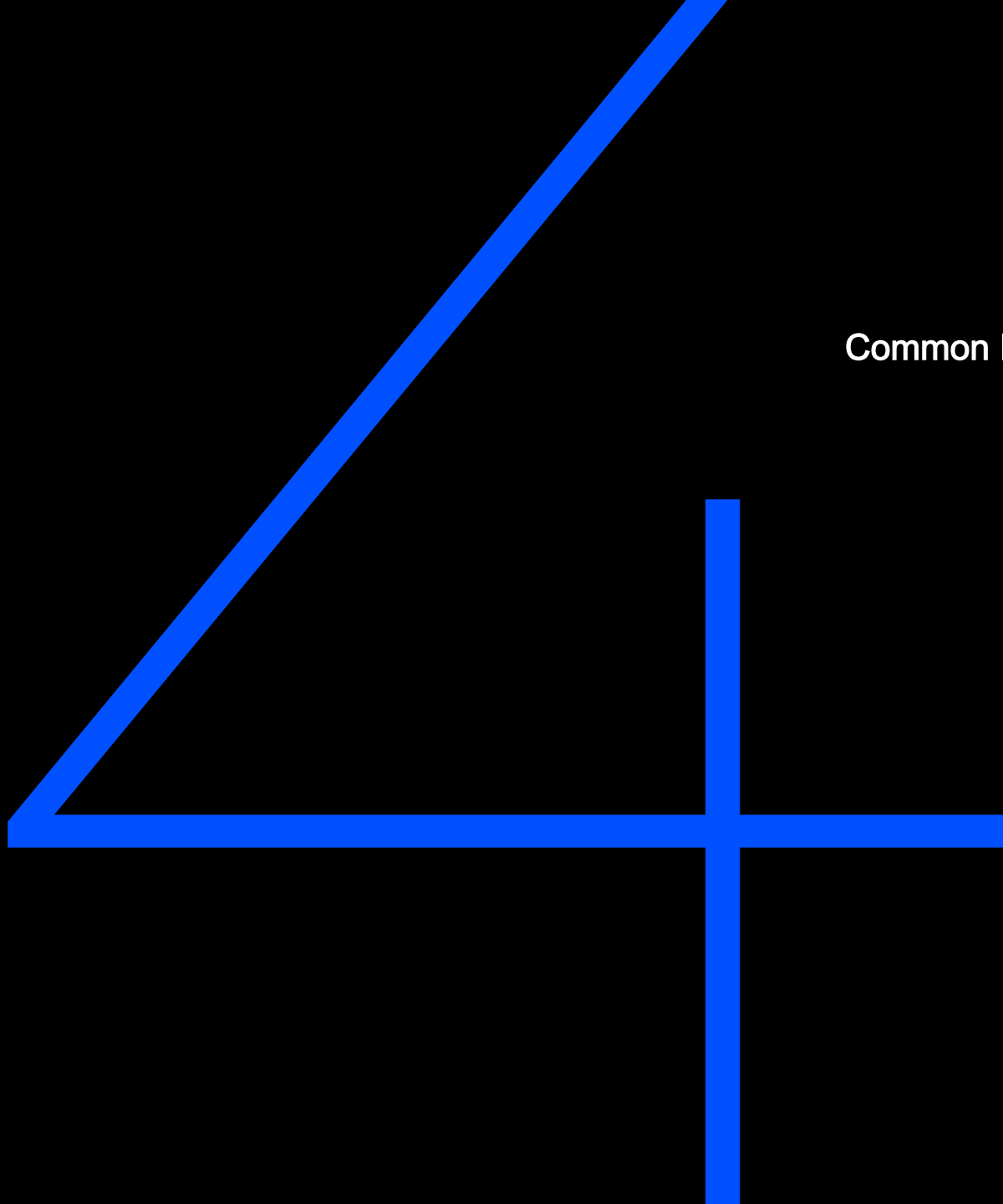
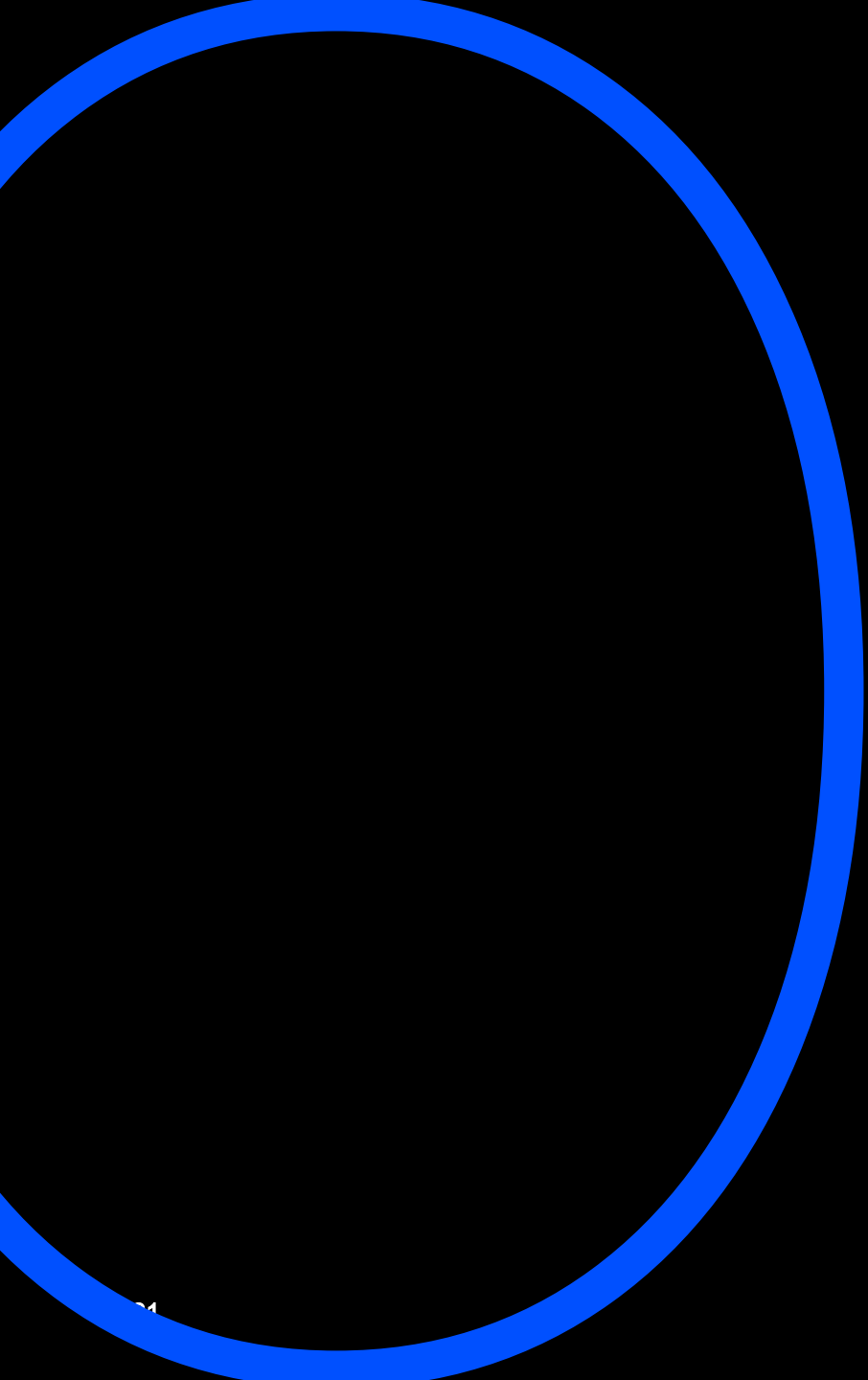
The mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.

# Poll 2

- **Comprehensive and Detailed Wire Transfer Policy & Procedures**
  - Board approved
  - Wire approval authorization
  - Methods in which a wire can be initiated
  - If a wire is not initiated in person – acceptable verification procedures
  - Member vs. Non -Member
  - Recurring Wires
    - Recurring Wires over the stated limits
  - Security controls
  - Segregation of Duties
  - Wire logs
  - Compliance with requirements under the Bank Secrecy Act including sanctions
  - Reconciliation of wire transactions
  - Verification of funds

- **Training & Cross Training**

- Regular and appropriate training for employees
  - Policy
  - Social Engineering
  - Fraud Awareness and prevention
  - Systems (use of technology)
  - Segregation of Duties: receiving, approving, inputting and releasing
  - Elder Abuse (romance schemes)
  - FedLine – annual requirements to review password policy and controls circular
  - Incident Response – how to escalate a suspect transaction



Common Findings

## **Common Audit Findings**

**Lack of Segregation of Duties**

**Inadequate Policies & Procedures**

**Inadequate Record Retention**

**Non -Compliance with  
Regulatory Requirements**

**Insufficient Training**

**Failure or Inadequate  
Monitoring or Reporting**

Q5

Nacha Rule Changes

- ACH Risk Management Topics

- Codifying expanded use of return reason code R17
- Expanded use of ODFI request for return R06
- Additional funds availability exceptions
- Timing of written statement of unauthorized debit
- RDFI must promptly return unauthorized debit.
- Fraud, monitoring by Originators, Third -party service providers/Third -party senders and ODFIs
- ACH Credit Monitoring by RDFIs
- Standard Entry Descriptions – PAYROLL and PURCHASE

- Minor Topics Rules Changes

- General Rule/Definition of WEB Entries
- Definition of Originator
- Originator action on notification of change
- Data security requirements
- Use of Prenotification entries
- Clarification of Terminology – Subsequent entries



## Codifying Use of Return Reason Code R17 (effective 10/1/24)

- Explicitly allows use of Return Reason Code R17
  - Optional and at the discretion of the RDFI
  - Must include **“QUESTIONABLE”** in the return addenda record

## Expanded Use of ODFI Request for Return – R06 (effective 10/1/24)

- Expands use of R06 to allow an ODFI to request a return from the RDFI for any reason
  - Use in cases of potential fraud
  - Still requires indemnity letter
  - RDFI compliance with request to return is optional

## Additional Funds Availability Exceptions (effective 10/1/24)

- An RDFI may delay funds availability if fraud of a credit entry where fraud is suspected
  - Allows additional time for participants to communicate before funds making funds available
  - Still need to comply with Reg CC

Timing of Written  
Statement of  
Unauthorized  
Debit (WSUD)  
(effective 10/1/24)

- WSUD can be signed and dated on or after date on which entry is presented to the Receiver, even if the debit has not yet posted to the account
  - Could be memo posted/pending transaction
  - May require additional training to front line staff

## RDFI Must Promptly Return Unauthorized Debit (effective 10/1/24)

- Return must be transmitted in time to be made available to the ODFI no later than the opening of business on the 6<sup>th</sup> banking day following the completion of review
  - Still have 60 -day return window overall
  - Allows for improved recovery of funds and reduced fraud

## Fraud Monitoring by Originators, Third Party Service Providers/Third Party Senders and ODFIs

- Requirement to establish and implement risk-based processes and procedures reasonably intended to identify ACH entries due to fraud
- Need to review at processes and procedures at least annually
- **Phase 1 – Effective March 20, 2026** – All ODFI's. As well as non-consumer Originators, Third Party Service Providers, and Third Party Senders with volume in excess of 6 million entries in 2023
- **Phase 2 – Effective June 22, 2026** – will apply to all other non-consumer Originators, Third Party Service Providers, and Third Party Senders

## RDFI ACH Credit Monitoring

- RDFI's will need to establish and implement risk-based processes and procedures to identify credit entries initiated due to fraud
- Need to review at processes and procedures at least annually
- Phase 1 – Effective March 20, 2026 –RDFI's with annual ACH receipt volume exceeding 10 million entries in 2023
- Phase 2 – Effective June 22, 2026 – will apply to all other RDFI's

## Standard Company Entry Descriptions

### PAYROLL and PURCHASE

- New Standard Company Entry Descriptions
- **PAYROLL** – Used for PPD credits for the payment of wages, salaries and other similar types of compensation
- **PURCHASE** – Used for e-commerce/online purchases which is defined as a debit entry authorized by a consumer Receiver for the online purchase of goods
- Effective March 20, 2026, but may begin using immediately



## Supplement #2 -2024

- Includes excerpts from the 2024 Nacha Operating Guidelines that have been updated to reflect key aspects of the new fraud monitoring rules
- Includes 2025 Network Administration Fees

## ACH Operations Bulletin #1 -2024: Changes to Upcoming Rules Effective Dates

- Provided clarification that upcoming rules with effective dates of June 19, 2026, have a practical effective date of June 22, 2026

# ACH Ops. Bltn. #2 -2024: Voluntary Formatting Standard for Individual Name Field

- Nacha recommends the following standard for the content of the Individual Name field:
  - LastName[space]AdditionalLastName[space]Suffix[space]FirstName[space]MiddleInitial[space]&[space]SecondaryReceiverFirstName[space]SecondaryReceiverMiddleInitial
  - If an Entry has two Receivers with different last names:  
LastName[space]AdditionalLastName[space]Suffix[space]FirstName[space]MiddleInitial[space]&[space]SecondaryReceiverLastName[space]SecondaryReceiverFirstName
- Individual name field is 15 or 22 positions depending on SEC type
  - May require truncation of name(s)

*Receiver's Name(s)*

Steven Jones

Steven E. Jones

Steven E. Jones, Jr

Steven E. Jones-Smith

Christopher H. Higginbotham

Chris H. Higginbotham Smith

Steven E. and Deborah L. Jones

Steve Jones and Debbie Smith

*Individual Name Field Contents:*

JONES STEVEN

JONES STEVEN E

JONES JR STEVEN E

JONES SMITH STEVEN E

HIGGINBOTHAM CHRISTOPH

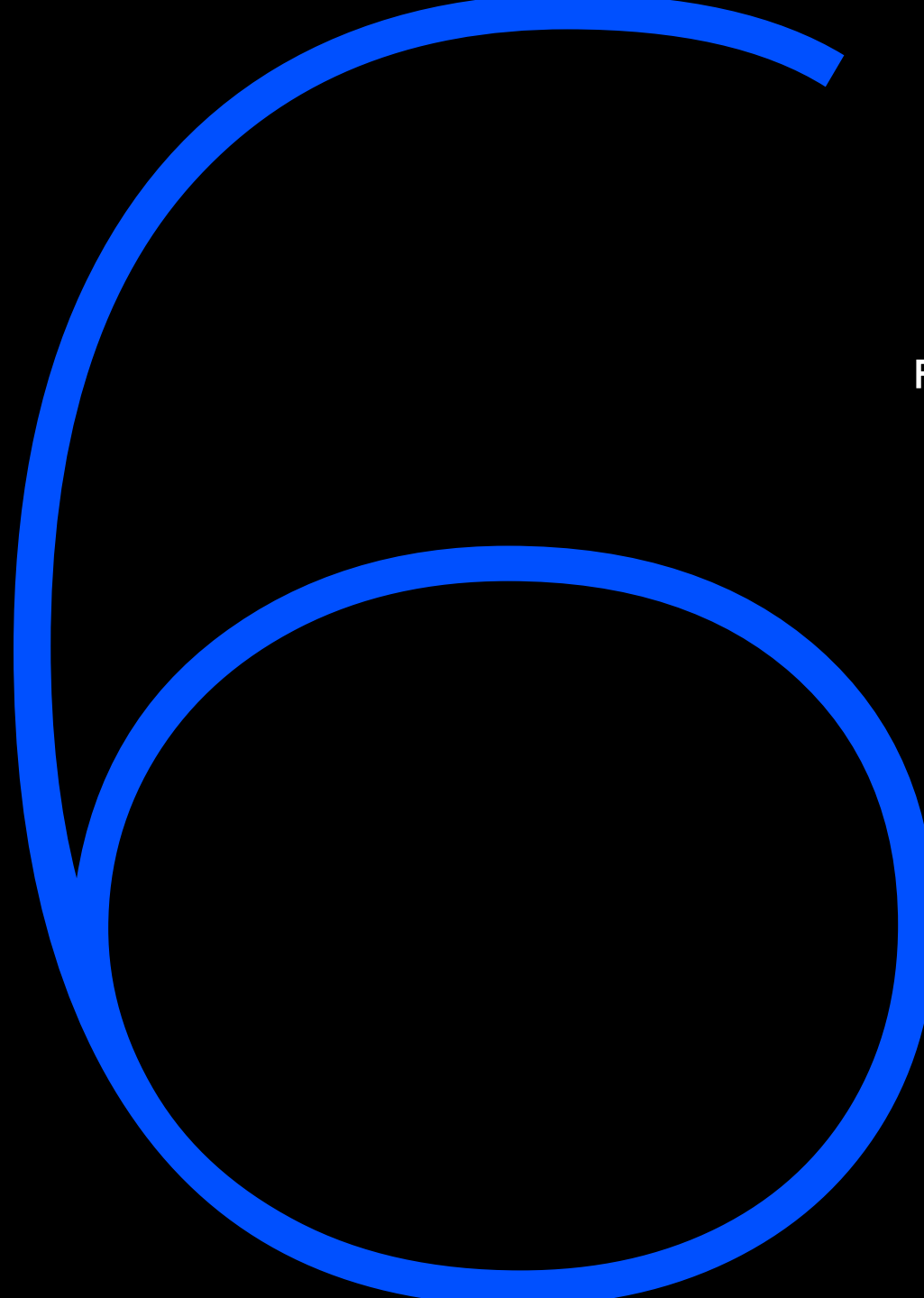
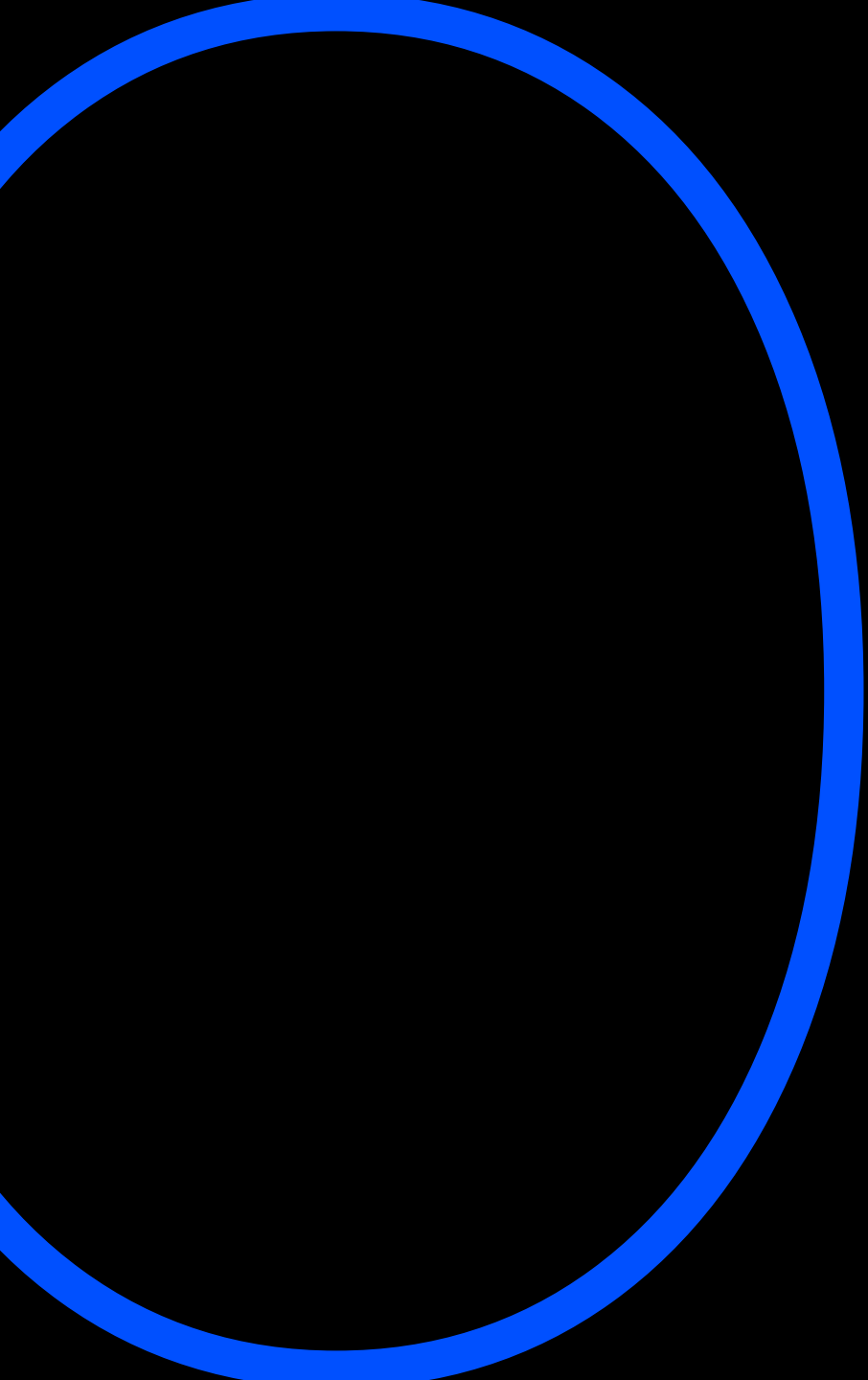
HIGGINBOTHAM SMITH CHR

JONES STEVEN E & DEBOR

JONES STEVE & SMITH DE

## ACH Operations Bulletin #3 -2024 -Open Banking and ACH Payments: The Impact of the CFPB's Personal Financial Data Rights Final Rule

- Provided guidance on the CFPB final rule implementing section 1033 of the Consumer Financial Protection Act



Fraud prevention

## RDFI's

- Train personnel AND customers on various types of fraud
- Respond promptly to any claims of unauthorized activity or fraud
- Software to monitor and flag unusual activity
- Consider use of Positive -pay for business customers

- Know your originators/third -party senders
  - Have identity verification and credit analysis procedures in place
  - Use Nacha's terminated originator database
  - Origination agreements should outline the roles of each party, be signed by both parties, and bind the originator to the rules
- Make sure your originators/TPS's understand the rules
  - Provide training
  - Keep them informed of rule changes
- Utilize dual controls
- Establish and periodically review exposure limits
- Consider use of micro -deposits and prenotifications

# • POLL 3





ACH - Originators

## Setting up new originators

- The ODFI should have a policy to risk rate, review, and approve each new originator
- All underwriting procedures should be documented
- Policies should be in place that define desirable and prohibited originators
- The ODFI should have a written credit policy to risk rate every originator or third party sender
- DOCUMENT ALL analyses performed

Examiners may want to see it

## Setting up new originators

- Credit analysis and background check should be performed prior to origination (and for ongoing due diligence)

Outsource to vendors (we do not profit from nor endorse any vendors), examples include

- Argos Risk (verify legitimacy, background check, comparative/analytical data)
  - [www.argosrisk.com](http://www.argosrisk.com)
- Dun & Bradstreet (verify legitimacy)
  - [www.dnb.com](http://www.dnb.com)
- LexisNexis (verify legitimacy)
  - [www.lexisnexis.com](http://www.lexisnexis.com)

## Setting up new originators

- Review sales history, tax returns, background checks
- Determine prefunding or collateral requirements
- Use of Nacha's terminated originator database (see page OR vi)
- Required: IDENTITY VERIFICATION (subsection 2.2.1)  
    Coincides with CIP (Customer ID Program) requirements

## Setting up new originators

- Nacha risk management advisory group

<https://www.nacha.org/content/rmag-risk-management-guidance>

- Sound Business Practices for Risk & Exposure Management

<https://www.nacha.org/news/rmag-sound-business-practices-risk-exposure-management>

## ODFI risk management practices

- Specifically, an ODFI is required to:

Perform due diligence with respect to originator/TPS sufficient to form a reasonable belief that the party has the capacity to perform its obligation in conformance with the Rules

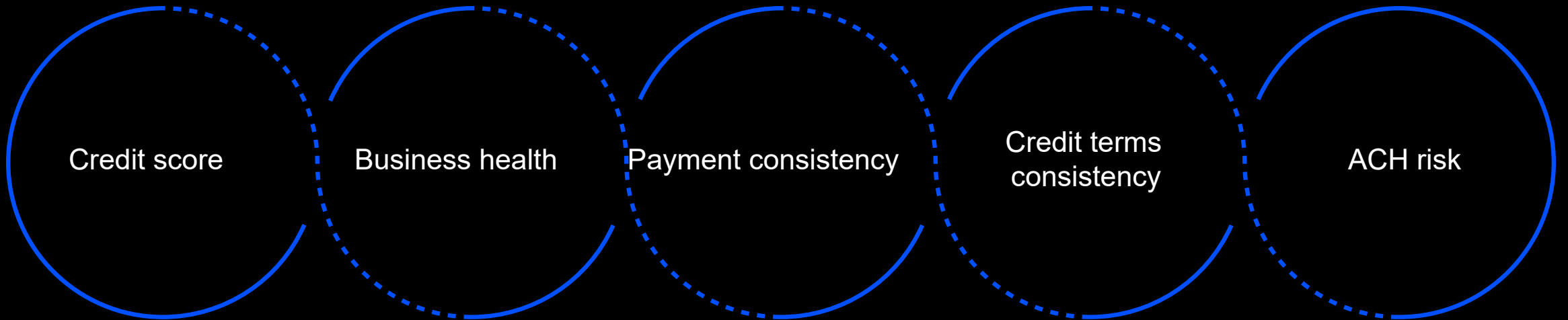
Assess the nature of the originator's/TPS's ACH activity and the risks it presents

Establish, implement, and review each exposure limit

Establish procedures to (1) monitor the originator's/TPS's origination and return activity, relative to its exposure limit, across multiple settlement dates; (2) enforce the exposure limit; and (3) enforce restrictions on the types of ACH transactions that may be originated. [See Section 2.2.3 of the ACH Rules]

# ODFI risk management practices

## Monitor business and transaction activity



## ODFI risk management practices

Due diligence should be performed and monitored for all areas for which the ODFI is liable

Authorization requirements

Entry/file setup and processing

Prenote origination compliance

NOC/return compliance

Business status and type

Purpose of entries



## Origination agreements requirements

—

- Nacha -required items for origination agreements are in Section 2.2.2 of the Nacha rules and include the following:

Originator must authorize ODFI to originate entries on behalf of the originator to the receivers' accounts

Originator must agree to be bound by the Nacha rules

Originator must agree not to originate entries that would violate the laws of the United States

## Origination agreements requirements

—

- Any restrictions on the types of entries that may be originated (this could also include SEC codes)
- The right of the ODFI to terminate or suspend the agreement for breach of the rules
- The right of the ODFI to audit the originator for compliance with the origination agreement and the rules

## Origination agreements

- The agreement may include the following information (Nacha -recommended)

The ODFI is indemnified against all claims and losses due to the originator's failure to perform its obligations under the rules

Processing schedules

Exposure limits (this is different from daily limits)

Procedures for exception handling (rejected, returned, and NOC entries)

## Origination agreements

- Arrangements for account funding for settlement and availability
- Procedures for re-transmittal of files
- Security procedures
- Contact names and authorized signers (must be current)
- Procedures for notification of data breach and implementation of commercially reasonable policies, procedures, and systems to detect the occurrence of a breach

## Origination agreements

- Appropriate warranty and liability provisions
- Any other items applicable as listed in the 2024 ACH Rules Book, page OG346-347, including but not limited to (these are often forgotten):
  - Nature: Purpose of the entries originated (ex: payroll, bill collection)
  - Format: The type of file to be sent (Nacha formatted file) and/or SEC code permitted (PPD, CCD, etc.)
  - Medium: How entries will be transmitted from the originator to the ODFI (Cash Management, encrypted email)
  - Debits/Credits/both: Reversals of the approved entry type are included

# Origination risk by SEC type

- The least amount of risk for an ODFI is to only originate PPD, CCD, CTX, or CIE entries
  - The other SEC codes require additional monitoring and risk to the FI
  - The board of directors should approve any other SEC types of ACH entries originated due to the increased risk of exposure

# Origination risk by SEC type

- Origination of SEC types other than CCD, CTX, and PPD need special attention by the ODFI
  - For what the originator wants to originate, ensure the correct SEC code is used (and offered by the ODFI)
  - Ensure proper security is in place for communication, data retention, destruction, etc.
  - Ensure all signs, disclosures, recordings, etc., are in place prior to origination
    - Receiver disclosures are a common error
    - The ODFI should review them prior to starting origination

## Originators' authorizations

- The ODFI ensures (warrants) that its originators comply with the following requirements:
  - Appropriate authorizations are obtained by the originator in accordance with the rules
  - Authorization has not been revoked or terminated
- Copies required to be provided to receivers
- Authorizations are retained for two years after termination as required by ACH rules



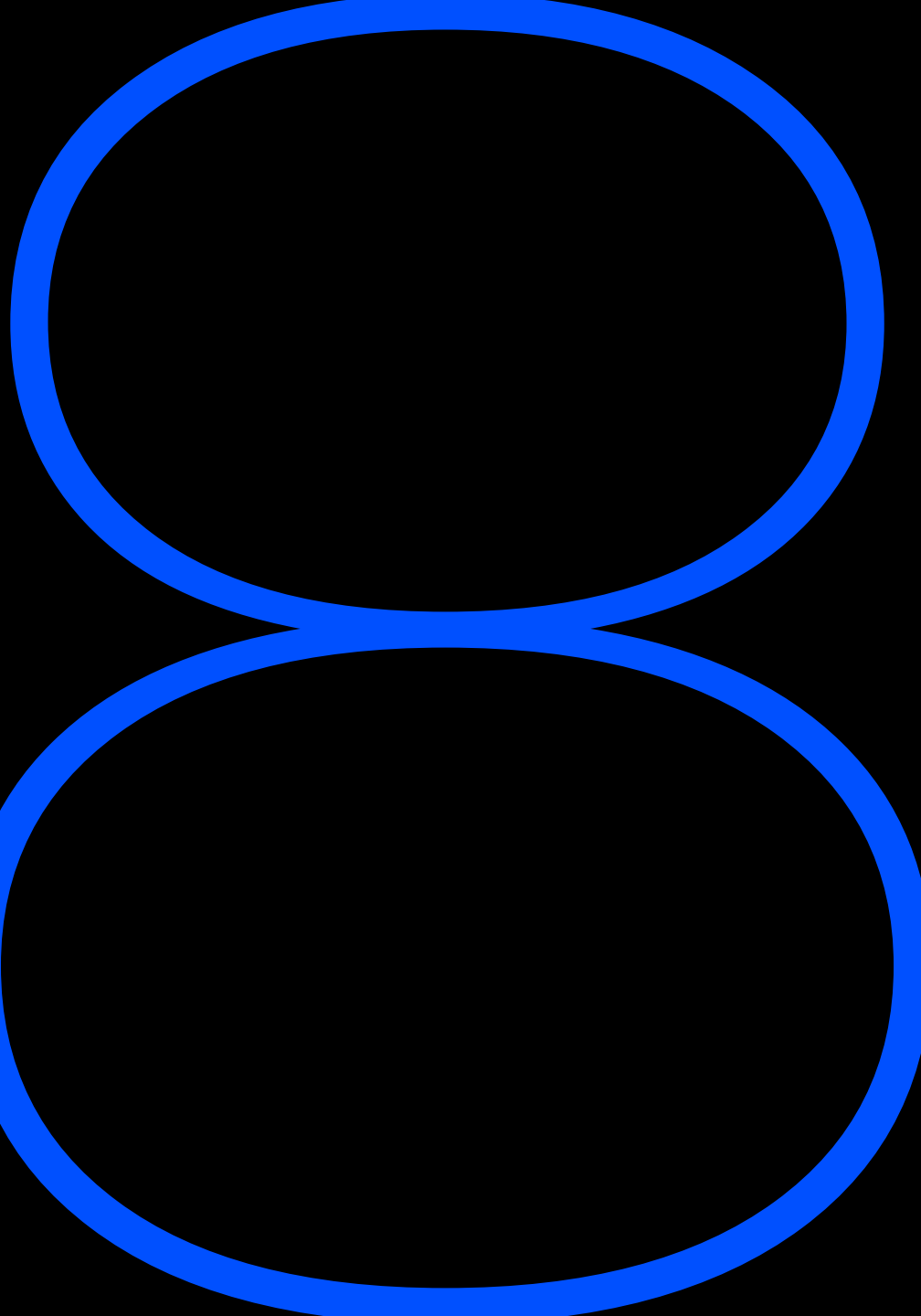
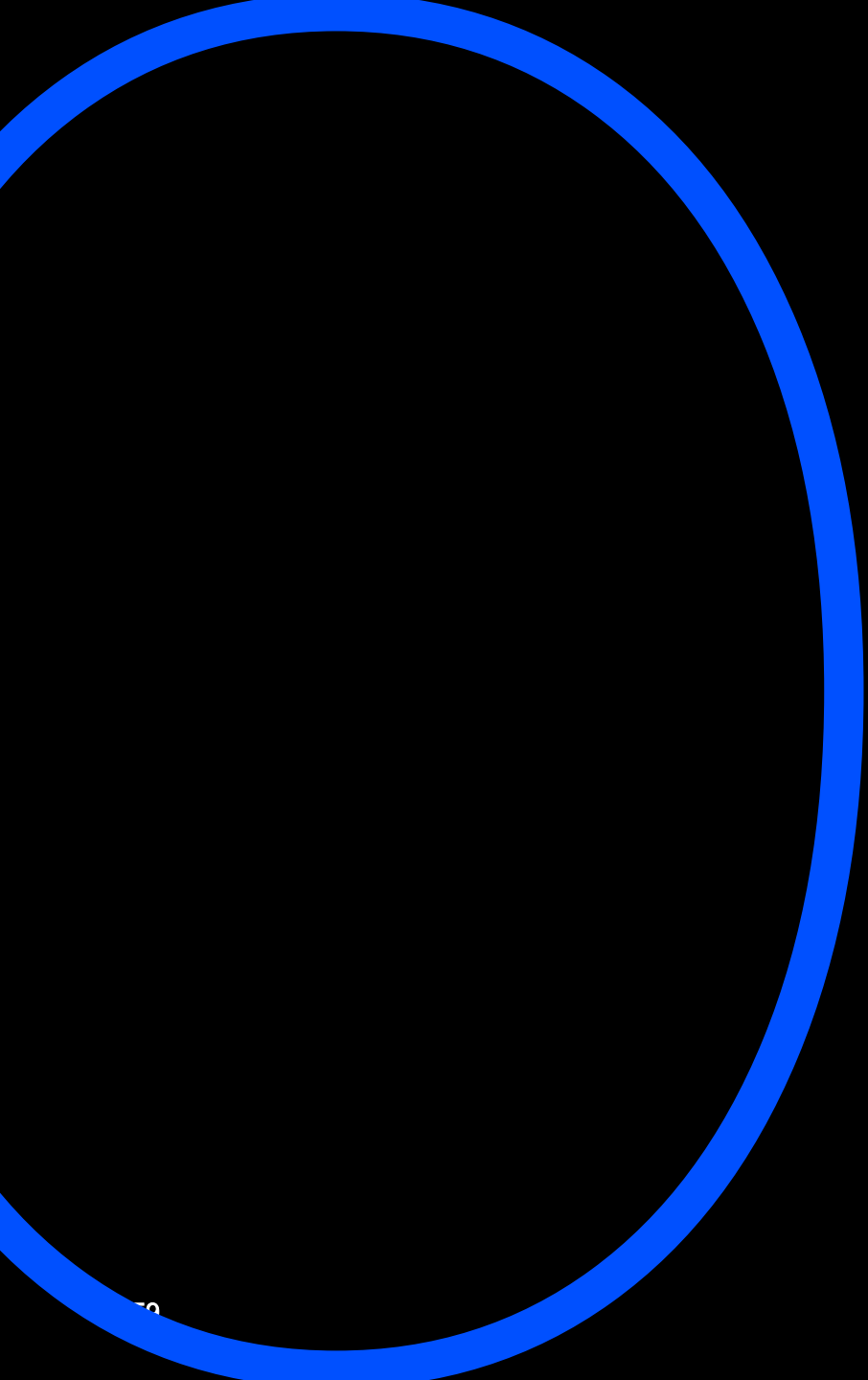
## Originators' authorizations

- While the FI is not required to “audit” their originators, the FI should remind originators of these requirements annually or as necessary to feel comfortable that the originators are complying

## Originators' authorizations

- While authorizations for credit entries are not required to be in writing, it is a good idea to have originators obtain them in writing

This reduces risk if there is a dispute or error



About Wipfli

Wipfli is a top advisory  
and accounting firm with  
55,900+ clients across every  
major industry.

A hand is shown pointing at a screen displaying a list of industries. The background is dark, and the hand is illuminated from the side, creating a strong contrast. The industries listed are: Manufacturing, Financial services, Construction, Real estate, Retail, Healthcare, Tribal gaming, Technology, Distribution, Agribusiness, Government, and Dealerships, Nonprofit.

## Industries

Manufacturing

Financial  
services

Construction

Real estate

Retail

Healthcare

Tribal gaming

Technology

Distribution

Agribusiness

Government

Dealerships

Nonprofit



**Our services**

---

Digital  
services

---

Risk  
advisory

---

Organizational  
performance

---

Outsourcing

---

Assurance

---

Tax services

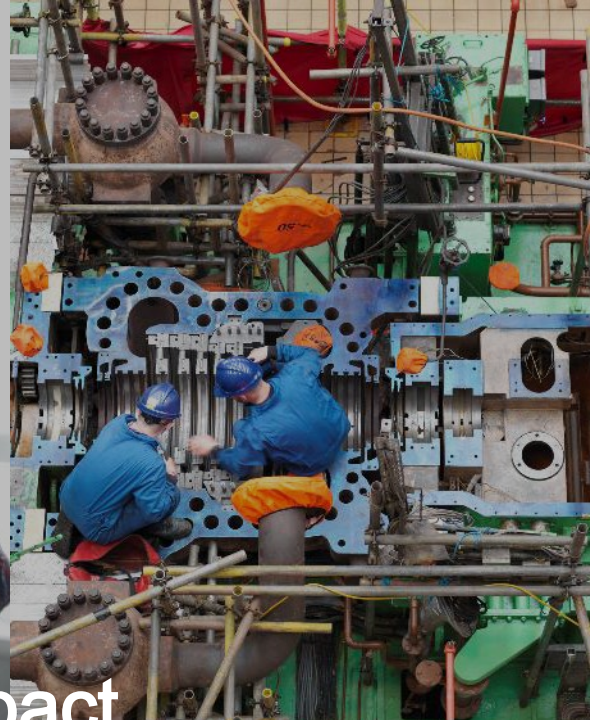
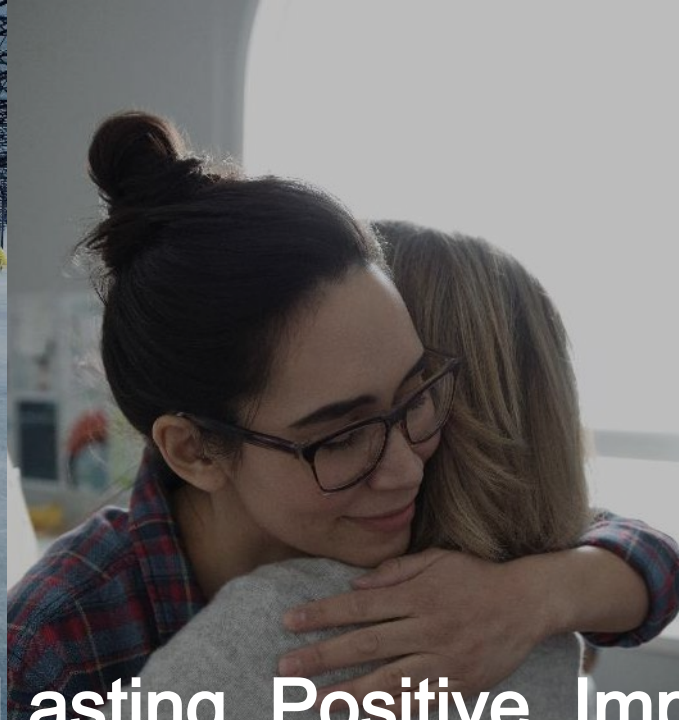
---

M&A transaction  
advisory

---

Private  
client services

Business consulting is what we do.  
*Why we do it is a different story.*



Lasting. Positive. Impact.





## Wipfli mission, vision and values

### Mission

To enable individuals and organizations to achieve their full potential, empowered by the security of a stable foundation.

### Vision

Create a lasting, positive impact for every person, organization and community we engage.

### Values

Integrity • Caring • Excellence • Teamwork • Perseverance

### Brand promise

Through deeply invested relationships and boundless curiosity, Wipfli brings clarity that drives results.

We seek to understand  
your business as deeply  
as you do.



Greater *understanding.*  
*engagement.*  
*impact.*  
*delivery.*  
*measurement.*  
*growth.*

Wipfli today

We have

3,300+

associates

We have

294

partners

We have

55,900+

clients

We achieved

\$590M


revenue in FY 2024

## Our commitment to diversity and inclusion

At Wipfli, we honor the unique strengths and contributions of every associate because we know that diversity makes us stronger.

Through initiatives focused on leadership, recruitment, training and diverse business resource groups, we will continue to become a more inclusive firm and build the workforce of the future.



A group of people, mostly young adults, are shown from behind, wearing blue t-shirts and hugging each other in a line. The scene is outdoors with a blurred background of trees and a fence. A solid blue rectangular box is overlaid on the left side of the image, containing white text.

With every step forward,  
we make a point  
to give back.


## #Wipfligivesback

### Community Day

While our passion for serving our communities is year-round, Community Day is a tradition established by Wipfli associates in 2005.

Every year, Wipfli associates from throughout the firm are given a day to spend volunteering and making a real difference in the communities where we work and live.





**ONE TEAM,**  
**ONE FOCUS.** **YOU.**