Faster Payments: The Journey from Authorization to Settlement

With the introduction of a variety of new, faster payment methods, including Same Day ACH, The Clearing House’s Real-Time Payment System (RTP) and Early Warning Services’ Zelle payment service, as well as a potential Federal Reserve Real Time Gross Settlement (RTGS) offering, the payments landscape is evolving rapidly.

These systems and services are subject to an extensive set of legal requirements. Those aiming to understand this legal framework must look to not only laws and regulations, but also payment system rules. Core laws include the Electronic Fund Transfer Act and its implementing regulation, Regulation E, and Article 4A of the Uniform Commercial Code (Article 4A). In many cases, the applicability and operation of these requirements, a financial institution’s obligations, and a customer’s rights, are dependent on the nature and features of a particular payment transaction. This includes, for example, whether the transaction is a consumer or commercial transaction; whether funds are moved via a “debit pull” payment or a “credit push payment”\(^2\); and whether the transaction is reversible or final. In many cases, these distinctions and their significance is not well understood. However, to make sense of the legal requirements for new, faster payments systems, it is essential to understand core payment concepts and how the functionality of these systems differ.

Payment System Operating Rules

At present, most new faster payments systems are governed by rules promulgated by the payment system operator or a designated rulemaking organization, such as the NACHA Operating Rules, Zelle Rules, and RTP Participation and Operating Rules.\(^3\) These rules set consistent expectations and operational requirements for the financial institutions that participate in a payment system. Such rules also serve as multilateral contracts that allow for scalability by removing the need for participants to enter into a contract with every other participant in the network. These rules supplement other laws and regulations, and in the case of 4A, may modify existing law. Another important function is to establish the allocation of loss among system participants, including with respect to unauthorized or erroneous payments. For example, under the NACHA Rules, the bank that initiates an ACH debit warrants that the transaction is authorized.\(^4\) Thus, the financial responsibility for unauthorized ACH debits generally falls on the payee’s bank as the payer’s bank may bring a breach of warranty claim against the payee’s bank.

---

2. These terms refer to how the payment is initiated and submitted to a payment system. In the debit pull model, the payment is initiated by the payee. The payee submits the transaction to a payment system to “collect” funds from the payer. In the credit-push model, the payment is initiated by the payer. The payer is “sending” funds to the payee.
3. The RTP Participation and Operating Rules are available here: [https://www.theclearinghouse.org/payment-systems/rtp](https://www.theclearinghouse.org/payment-systems/rtp).
4. NACHA Operating Rules, Subsection 2.4.1.1
Legal Requirements

In addition to contractual rules governing participation, new faster payments systems and their participants are still subject to existing legal obligations, particularly with respect to protecting consumers against erroneous and unauthorized transactions. The limitation of liability and error resolution requirements of the EFTA and Regulation E are applicable to erroneous and unauthorized consumer payments conducted through Same Day ACH, Zelle and RTP. Under Regulation E consumers may notify their financial institution of errors (as defined in the regulation) within 60 days of the periodic statement that reflects the error. If notified of the error within the appropriate timeframe, a financial institution must investigate the error, report the results of its investigation to the consumer, and correct the error if it is determined that an error occurred. Accordingly, if a consumer claims that an error has been made with respect to a Same Day ACH, Zelle or RTP Payment, the consumer’s financial institution must investigate the error, report the results of the investigation, and correct any error.

The requirements of Article 4-A of the New York Uniform Commercial Code apply with respect to erroneous or unauthorized transactions that are not subject to the EFTA, and apply to both commercial RTP transactions and commercial Same Day ACH credits. Article 4-A allocates responsibility for various errors between the parties to a funds transfer. With respect to commercial Same Day ACH credits (but not debits) and commercial RTP transactions, liability as between the payer and the payer’s financial institution will be determined based upon Article 4-A’s security procedure framework.5

The application of these legal requirements, and the ultimate allocation of loss for an erroneous or unauthorized transaction differs based on the nature of the payment and in particular, whether it is a debit or credit transaction. For example, in a credit push system like RTP, the payer’s financial institution will have Regulation E obligations for unauthorized transactions from a consumer payer’s account. This obligation is independent of whether the consumer’s financial institution is able to recover funds from the payee’s financial institution. In other words, the financial responsibility for unauthorized RTPs falls to the sending financial institution. At a high level, the principle underlying this approach is that the payer’s financial institution should bear the loss because it is responsible for authenticating its customer and submitting the payment into the system, while the payee’s financial institution has simply received the transaction in a passive role. This is in contrast to debit-pull payment systems in which the payee’s financial institution (originates the debit into the system) will generally have an obligation to repay another financial institution for an unauthorized transaction (through return or charge back rights) to a customer’s account at that institution. This includes, for example, the NACHA authorization warranty referenced above.

Evolving Regulatory Expectations

Unsurprisingly, regulators are paying close attention to these new payment services and systems. Notably, the CFPB has identified certain “long term actions” that are “potential rulemakings” to begin “beyond the immediate next 12 month period.” The list includes a “Regulation E modernization” effort to address, among other things, issues raised by new payment systems. The notice states that “[n]ew payment

5 See UCC 4-A-201 through 4-A-204.
systems are emerging, and many existing electronic fund transfer systems have undergone substantial changes since the initial implementation of EFTA. Technologies and business practices have evolved, creating new questions about adapting consumer protections to new channels and circumstances, potential relief from outdated provisions, and other issues.” The fact that the CFPB intends to consider and address how “providers of new and innovative products and services comply with regulatory requirements” suggests the Bureau may update disclosure provisions and error resolution requirements.

Further, in September 2018, the CFPB released a blog post that describes new mobile payment services and provides tips for consumers to protect themselves from scams, misdirected payments and other problems associated with credit push/irrevocable payments. The post may provide some clues about the CFPB’s thinking as it moves forward with its “Regulation E modernization” effort. For example, the post suggests that the CFPB may be considering steps to address scenarios that are not currently covered by Regulation E, such as payments that a consumer authorizes, but was “tricked” into making by a fraudster, or payments made to an unintended recipient where the consumer has provided incorrect routing information. The post also includes an invitation to consumers to report problems with payment services to the CFPB through their consumer complaint process. Thus, as consumer use of new payment services increases, their concerns and complaints to the CFPB are likely to inform the agency’s future regulatory actions to modify existing consumer rights and the related requirements for financial institutions.

---

Faster Payments: The Journey From Authorization to Settlement

Presented by the ABA Payments and Electronic Banking Subcommittee

CLE MATERIALS

LAUREN GILES, ALSTON & BIRD
PAUL HOLBROOK, HSBC BANK USA, N.A.
STEPHEN KREBS, THE CLEARING HOUSE

03.29.19
Overview

This CLE program will explore the legal framework applicable to faster payments, including Regulation E, UCC Article 4-A, and payment system operating rules.

The panel will cover the features and functionality of faster payment systems and will use specific examples and hypotheticals to explain core payments law principles and the roles that various parties may play in an overall transaction.
Disclaimer

- The views expressed during this presentation are the presenters’ own and should not be attributed to their employers or considered legal advice.
Topics

- **Introduction**
  - Key Payments Concepts
  - Electronic Payments Fraud and Errors
  - Faster Payments Landscape

- **Legal Requirements**
  - Core US Laws and Regulations Applicable to Electronic Payments, including Faster Payments
  - Key Payment Network Rules

- **Hypotheticals**

- **Evolving Regulatory Expectations**
Key Payments Concepts

- **“Debit Pull” vs. “Credit Push”**
  - Refers to how the payment is initiated and submitted to the payment system
  - Why it matters: the risks and legal liabilities (for both customers and financial institutions) vary significantly
“Debit Pull”

• In the debit pull model, the payment is initiated by the payee

• The payee submits the transaction to a payment system to “collect” funds from the payor

• Increased risks: insufficient funds, returned transactions, unauthorized transactions

• Examples: checks, cards, ACH debits
“Credit Push”

• In the credit-push model, the payment is initiated by the payor.

• The payor is “sending” funds to the payee

• Fundamentally safer -- the payor’s bank is responsible for authenticating the payor and confirming that “good funds” are available for the transaction, so there is no risk of insufficient funds

• Examples: wire transfers, ACH credits, RTP, Zelle
Key Payments Concepts

- Key steps in an electronic payment
  - **Authorization**: account-holding customer authorizes a payment from his or her account
  - **Clearing**: exchange of information/commitment to pay through payment networks that allow the payor and payee’s financial institutions to update their accounts
  - **Settlement**: the discharge of the obligation of the payor’s financial institution to the payee’s financial institution through the transfer of funds
Introduction to Electronic Payment Errors and Fraud

- Unauthorized transactions vs. scams
  - Unauthorized (payor did not authorize the payment from his/her account)
    - Examples include account takeover, debit by a payee that did not obtain payor’s authorization
  - Scams (payor fraudulently induced to make an authorized payment)
    - Examples include business email compromise, fraudulent seller that does not deliver goods

- Errors
  - Bank error
    - Examples include misrouted payment to wrong payee, incorrect payment amount, duplicate payment
  - Customer error
    - Examples include customer provides bad payee information
Distinction Between Consumer Rights and Interbank Obligations

- Regulation E governs relationship between financial institution and customer.
  - A financial institution has Regulation E obligations to its customer regardless of whether it is able to recover funds from another financial institution involved in the transactions.

- Payment system rules may allocate responsibility for the loss between financial institutions.
  - For example, in a debit-pull payment system a financial institution that originates an unauthorized debit will generally have an obligation to repay another financial institution (through return or charge back rights) whose customer’s account was debited without authorization.
Faster Payments Landscape

- Industry Led Faster Payment Initiatives
  - TCH Real-Time Payments (RTP)
  - EWS Zelle
  - NACHA Same Day ACH

- What’s the Difference?
  - Same Day ACH (new rules that enhance an existing payment system to establish additional settlement windows and faster funds availability)
  - RTP (new payment system, i.e., payment “rails”)
  - Zelle (new payment service)

- Functions and Features
  - Same Day ACH includes debits; delayed settlement
  - RTP and Zelle are credit push only
    - Zelle clears nearly immediately, but generally settles via ACH
    - RTP clears and settles immediately
Sources of Legal Requirements for Electronic Payments

- Core US Laws Applicable to Electronic Payments, *including Faster Payments*
  - Electronic Fund Transfer Act & Regulation E (consumer)
  - UCC 4A (non-consumer)

- Other Core Sources of Legal Requirements Applicable to Faster Payments
  - Payment Network Rules
    - RTP Rules
    - Zelle Rules
    - NACHA Rules
Regulation E

- Regulation E protects consumers against unauthorized transfers and other bank errors.

- The definition of “error” includes an unauthorized electronic fund transfer, and an incorrect electronic fund transfer to or from the consumer's account. 12 CFR § 1005.11(a)(1).

- However the definition of error does not include:
  
  - Fraudulently induced payments (scams)
  
  - Payments routed based on wrong information provided by sender.
Regulation E (continued)

- Under Regulation E consumers must notify their financial institution of errors within 60 days of the periodic statement that reflects the error.

- If notified of the error within the appropriate timeframe, a financial institution must:
  - investigate the error,
  - report the results of its investigation to the consumer, and
  - correct the error if it determines that an error occurred.
The Sending customer is not liable to the sending bank for a funds transfer if the transfer is not authorized by the customer. (UCC 4A-202)

- A funds transfer is deemed “authorized” by the sending customer if the sending bank verified the authenticity of the instruction with a “security procedure”.

- The security procedure must be “commercially reasonable” and the bank must have acted in “good faith.”
UCC Article 4A – Security Procedure

- 4A-201 Security Procedure:
  - “a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or
  - (ii) detecting error in the transmission or the content of the payment order or communication."

- “The question of whether loss that may result from the transmission of a spurious or erroneous payment order will be borne by the receiving bank is affected by whether a security procedure was or was not in effect and whether there was or was not compliance with procedure.” UCC Official Comment to 4A-201
UCC Article 4A – Security Procedure

• What security procedures are in general use by depository institutions?

• FFIEC Guidance (2005) - “Authentication in an Internet Banking Environment” (Supplemented 2011)

• Some courts have viewed this as industry standard- not a recommendation

• Risk assessments should be done annually and prior to installation of any new electronic banking system

• For “high-risk” Commercial transactions:
  o (i) implement layered security controls,
  o (ii) offer multifactor authentication, and
  o (iii) enhance controls for system administrators

• Layered security controls - include anomaly detection and response at:
  o (i) initial customer login, and
  o (ii) initiation of funds transfer to other parties.

• Simple device identification & simple challenge questions are not enough

• Provide Customer awareness and education training
UCC Article 4A

- Other UCC 4A provisions relevant to unauthorized and erroneous transfers
  - § 4A-204. Refund of payment and duty of customer to report with respect to unauthorized payment order
  - § 4A-205. Erroneous payment orders
  - § 4A-207. Misdescription of beneficiary
Other Sources of Requirements

- Payment System Rules:
  - supplement, and in the case of 4A, may modify existing law
  - set consistent expectations and operational requirements for system participants (financial institutions)
  - establish the allocation of loss among system participants, including with respect to unauthorized/erroneous payments
    - Examples: authorization warranties, chargeback rights
  - serve as multilateral contracts that allow for scalability by removing the need for participants to enter into a contract with every other participant
With respect to unauthorized transfers and errors, as between the financial institution and its customer:

- Regulation E governs consumer payments
- UCC 4A governs commercial payments

**RTP Rules**

- Participants are required to reasonably cooperate among themselves and with TCH in attempts to address and recover erroneous RTP Payments. *See RTP Operating Rule II.I.3.*
- A Participant may submit a Request for Return of Funds for any reason, including to request a return of funds related to an erroneous RTP Payment or an RTP Payment made in response to a fraudulent Request for Payment. However, the Receiving Participant is under no obligation to return the funds.
RTP Legal Framework – Errors/Unauthorized Transactions (Consumer)

- **Application of Regulation E**

  - As RTP is a credit push-payment system, claims of unauthorized RTPs, which are errors for purposes of Regulation E, would be made by the Sender.

  - The Sending Participant, which allowed the payment to be sent, would have an obligation to investigate, report, and credit the Sender, if the payment was in fact unauthorized.

  - The Sending Participant may use the Request for Return of Funds message. However, the Sending Participant’s Regulation E obligations are not dependent on whether the Receiving Participant returns the funds.
RTP Legal Framework – Errors/Unauthorized Transactions (Commercial)

- The requirements of Article 4-A of the New York Uniform Commercial Code apply with respect to erroneous or unauthorized transactions that are not subject to the EFTA. Article 4-A allocates responsibility for various errors between the parties to a funds transfer.

- With respect to unauthorized RTPs, liability as between the Sender and the Sending Participant will be determined based upon Article 4-A’s security procedure framework.

- Again, while RTP provides a Request for Return of Funds message, this RTP capability does not alter a Sending Participant’s Article 4-A obligation to the Sender with respect to an unauthorized RTP payment.
With respect to unauthorized transfers/errors (as between the financial institution and its customer), the following apply:

- Regulation E (consumer credits and debits)
- UCC 4A (non-consumer credits)

The NACHA Rules establish requirements between financial institutions participating in the ACH system

- Interbank warranties that ACH transactions are authorized. NACHA Operating Rules, Subsection 2.4.1.1
- Thus, the financial responsibility for unauthorized ACH debits generally falls on the payee’s bank as the payor’s bank may bring a breach of warranty claim against the payee’s bank.
Faster Payments - Hypotheticals

- **HYPOTHETICALS** – to be shared at time of presentation
Evolving Regulatory Expectations

- The CFPB has identified certain “long term actions” that are “potential rulemakings” to begin “beyond the immediate next 12 month period.”

- The list includes a “Regulation E modernization” effort to address, among other things, issues raised by new payment systems.

- The notice states that “[n]ew payment systems are emerging, and many existing electronic fund transfer systems have undergone substantial changes since the initial implementation of EFTA. Technologies and business practices have evolved, creating new questions about adapting consumer protections to new channels and circumstances, potential relief from outdated provisions, and other issues.”

- The CFPB intends to consider and address how “providers of new and innovative products and services comply with regulatory requirements” indicates it may update disclosure provisions and error resolution requirements.
In September 2018, the CFPB released a blog post that describes new mobile payment services and provides tips for consumers to protect themselves from scams, misdirected payments and other problems associated with credit push/irrevocable payments.

The post may provide some clues about the CFPB’s thinking as it moves forward with its “Regulation E modernization” effort.

The post also includes an invitation to consumers to report problems with payment services to the CFPB through their consumer complaint process.