

CONSUMER COMPLIANCE OUTLOOK®

A FEDERAL RESERVE SYSTEM PUBLICATION FOCUSING ON CONSUMER COMPLIANCE TOPICS

INSIDE

Error Resolution Procedures Under the Electronic Fund Transfer Act and Regulation E..... 2

Consumer Liability for Unauthorized Transactions Under the Electronic Fund Transfer Act and Regulation E..... 6

Error Resolution Under Regulation E: Examiner Insights and Common Violations..... 12

Regulatory Calendar.....18

THE ELECTRONIC FUND TRANSFER ACT, REGULATION E, AND INSTANT PAYMENT SERVICES

KENNETH BENTON, PRINCIPAL CONSUMER REGULATIONS SPECIALIST, FEDERAL RESERVE BANK OF PHILADELPHIA

To address the growing demand for faster payments, The Clearing House (TCH) introduced its RTP instant payment service in 2017, and the Federal Reserve introduced its FedNow instant payment service in 2023. These services allow participants to make instant payments 24 hours a day, 365 days a year. For example, a consumer can schedule a payment on its due date to avoid a late fee, or an employer can provide earned wage access payments to enhance recruitment and retention. As the number of institutions participating in FedNow and RTP continues to increase, it is important for participants to understand the legal framework for these services to ensure compliance. This article provides a brief history of electronic payments, discusses the FedNow and RTP services, and reviews the legal framework.

ELECTRONIC PAYMENT HISTORY

The Automated Clearinghouse Network

In the 1970s, the Federal Reserve and the banking industry developed the automated clearinghouse (ACH) network to facilitate electronic batch payments and reduce the need for paper checks.¹ After this network was created, the Federal Reserve began providing batch-based ACH transfers to government and private parties through its FedACH service, while TCH began providing batch-based ACH transfers to private parties through its Electronic Payment Network (EPN).² Nacha administers the ACH Network, which includes promulgating the rules for ACH transfers.³

While FedACH and EPN provided faster payment rails than checks, both services had limitations. They were available only Monday through Friday during specified hours, did not operate on federal holidays, and took one to three business days to complete transfers.

Same-Day ACH

To address these limitations, the Federal Reserve introduced its same-day FedACH service in 2010. This service provides same-day processing and settlement for payments initiated before specified cutoff times and on days the ACH operates.⁴ Similarly, Nacha introduced its same-day ACH service in 2016 to provide same-day transfers for payments initiated before specified cutoff times and on the days the ACH operates.⁵ Higher fees apply for these same-day services.

CONTINUED ON PAGE 15

**Consumer Compliance Outlook
Advisory Board**

Karin Bearss
Vice President, SRC
Federal Reserve Bank of Minneapolis

Matthew Dukes
Counsel, Policy/Outreach
Federal Reserve Board

David Kovarik
Assistant Vice President, BS&R
Federal Reserve Bank of Chicago

Robin Myers
Vice President, SRC
Federal Reserve Bank of Philadelphia

Andrew Olszowy
Vice President, SRC
Federal Reserve Bank of Boston

Contributors

Kathleen Benson
Federal Reserve Bank of Chicago

Kate Loftus
Federal Reserve Bank of Minneapolis

Scott Sonbuchner
Federal Reserve Bank of Minneapolis

Staff

Editors..... Kenneth Benton
Maura Fernbacher

Designer..... Monica Conrad

Project Manager..... Marilyn Rivera

Consumer Compliance Outlook is distributed to state member banks and bank and savings and loan holding companies supervised by the Board of Governors of the Federal Reserve System.

Disclaimer: The analyses and conclusions set forth in this publication are those of the authors and do not necessarily indicate concurrence by the Board of Governors (Board), the Federal Reserve Banks, or the members of their staffs. Although we strive to make the information in this publication as accurate as possible, it is made available for educational and informational purposes only. Accordingly, for purposes of determining compliance with any legal requirement, the statements and views expressed in this publication do not constitute an interpretation of any law, rule, or regulation by the Board or by the officials or employees of the Federal Reserve System.

Copyright 2025 Federal Reserve Banks. This material is the intellectual property of the 12 Federal Reserve Banks and cannot be copied without permission. To request permission to reprint an article, contact us at outlook@phil.frb.org.

ERROR RESOLUTION PROCEDURES UNDER THE ELECTRONIC FUND TRANSFER ACT AND REGULATION E

BY KENNETH BENTON, PRINCIPAL CONSUMER REGULATIONS
SPECIALIST, FEDERAL RESERVE BANK OF PHILADELPHIA

Editor's Note: In 2012, *Consumer Compliance Outlook (CCO)* reviewed the procedures financial institutions must follow under the Electronic Fund Transfer Act (EFTA) and Regulation E when consumers allege an error occurred in an electronic fund transfer (EFT) from or to their account. The article also discussed a consumer's potential liability under the EFTA and Regulation E when the error is an unauthorized EFT.¹ *CCO* is updating this article to reflect the 2016 final rule to provide Regulation E coverage of prepaid accounts and to discuss the requirements of an error resolution investigation.²

Part 1 of this two-part updated article discusses error resolution, and Part 2 discusses liability for unauthorized transactions. An article on page 1 discusses how the EFTA and Regulation E apply to instant payment services introduced by The Clearing House in 2017 and the Federal Reserve System in 2023.

ERROR RESOLUTION PROCEDURES 12 C.F.R. §1005.11

Congress passed the EFTA³ in 1978 to protect consumers engaging in EFTs by providing "a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems."⁴ The scope of the EFTA, as implemented by the CFPB's Regulation E (12 C.F.R. Part 1005), includes transactions involving automated teller machines (ATM), point-of-sale debit cards, certain government benefit accounts,⁵ direct deposits, gift cards, payroll cards, prepaid accounts,⁶ and foreign remittance transfers.⁷

Regulation E includes specific procedures that financial institutions⁸ must follow when consumers allege an error. Section 1005.11(a) defines *error* to include:

- an unauthorized EFT;
- an incorrect EFT to or from a consumer's account;
- an omission of an EFT from a consumer's periodic statement;
- a computational or bookkeeping error by the institution for an EFT;
- an electronic terminal's disbursement of an incorrect amount of money;⁹
- an EFT that was not identified in accordance with §1005.9 or §1005.10(a); and
- the consumer's request for documentation required by §1005.9 or §1005.10(a) or for additional information or clarification concerning an electronic fund transfer, including a request the consumer makes to determine whether one of the errors listed above exists.

To clarify the definition of *error*, the regulation specifies it does *not* include:

- routine inquiries about a consumer's account balance,
- requests for information for tax or other recordkeeping purposes, or

- requests for duplicate copies of documentation.¹⁰

A financial institution must follow the required error resolution procedures even if it receives notice of an error after the consumer has closed the account.¹¹

NOTICE OF ERROR REQUIREMENTS

A financial institution must comply with the error resolution procedures specified in §1005.11 for any notice of an error from the consumer that:

- is received by the institution no later than 60 days after transmitting the periodic statement on which the error is first reflected;¹²
- enables the institution to identify the consumer's name and account number;¹³ and
- indicates why the consumer believes an error exists and includes, to the extent possible, the type, date, and amount of the error.¹⁴

Consumers can provide either written or oral notice. If a consumer provides oral notice, the institution may require the consumer to provide written confirmation of the error within 10 business days after the oral notice.¹⁵ The Official Staff Commentary for Regulation E clarifies that “the error resolution procedures ... apply when a notice of error is received from the consumer, and not when the financial institution itself discovers and corrects an error.”¹⁶

INVESTIGATION

Timing of an Investigation

An investigation must begin *promptly* after the receipt of an oral or written notice of an error.¹⁷ When the error is an unauthorized EFT, one related issue is whether an institution may impose conditions *before* it will begin an investigation, such as requiring the consumer to first dispute the transaction with the merchant or file a police report. The Official Staff Commentary states that an institution may *not* delay its investigation pending receipt of information from the consumer.¹⁸

Burden of Proof

When the alleged error is an unauthorized EFT, the EFTA places the burden of proof on the financial institution to establish that the transaction was authorized. Therefore, if the institution cannot establish that the disputed EFT transaction was authorized, the transaction is considered an unauthorized EFT, and the institution must correct the error in accordance with the liability limits in §1005.6.¹⁹

To mitigate this risk, a financial institution's compliance department can conduct transaction testing on previously

denied error notices. For each previously denied allegation within the selected sample, the institution can confirm that employees reviewed all relevant information within the institution's records and that the findings of the investigation met the institution's burden of proof to establish that an error did not occur. If the transaction testing revealed that the institution was not adhering to regulatory requirements, it could enhance its internal controls by, for example, providing additional training to the staff handling the investigations.

Investigation Must Be Reasonable

A financial institution cannot deny a consumer's claim of an error without conducting a *reasonable investigation*.²⁰ However, a financial institution may forgo an investigation if it corrects the error as the consumer has alleged (and complies with all other applicable requirements of §1005.11).²¹ A *reasonable investigation* includes reviewing relevant information within the institution's records when the alleged error concerns a transfer with a third party, and the institution does not have an agreement with that party for the type of EFT involved.²² The Official Staff Commentary provides that the information that may be reviewed may include:

- the ACH transaction records for the transfer;
- the transaction history of the account for a reasonable time period immediately before the allegation of error;
- whether the check number of the transaction in question is notably out of sequence;
- the location of the transaction or the payee in question relative to the consumer's place of residence and usual transaction area;
- information relative to the account within the control of the institution's third-party service providers if the financial institution reasonably believes that it may have records or other information that could be dispositive of the consumer's alleged error; or
- any other information appropriate to resolve the claim.²³

This comment also clarifies that “the investigation required may vary depending on the facts and circumstances. However, a financial institution may not limit its investigation solely to the payment instructions where additional information within its own records pertaining to the particular account in question could help to resolve a consumer's claim.”²⁴

TIME LIMITS FOR COMPLETING INVESTIGATIONS

Generally, a financial institution must finish investigating an error within 10 business days of receiving a notice of the error, but it can extend the period to 45 calendar days if it cannot complete the investigation within the 10-day period and it satisfies certain requirements.²⁵ In certain

circumstances, the 10-day period can be extended to 20 days and the 45-day period can be extended to 90 days.

10 Business Days After Notice: Unless a financial institution is permitted a longer time period to investigate an error in the circumstances described next, the institution has 10 business days after receiving notice from the consumer to investigate if an error occurred.

20 Business Days After Notice Exception: If the alleged error involves an EFT within 30 days after the first deposit into the account, the investigation period is extended to 20 business days instead of 10.²⁶

45 Calendar Days After Notice Exception: If the financial institution is unable to complete its investigation within 10 business days, it may extend the period to 45 calendar days from the receipt of the error notice, provided that the institution:

- provisionally credits the consumer's account for the full amount of the alleged error plus interest, if any. However, the institution may withhold a maximum of \$50 of the amount credited if the institution has a "reasonable basis" for believing an unauthorized EFT occurred and complies with the limitation on liability rules in §1005.6(a), which are discussed in the companion article on a consumer's liability for unauthorized EFTs on page 6.
- informs the consumer of the amount and date of the provisional crediting within two business days of the crediting; and
- allows the consumer full use of the provisional funds during the investigation.²⁷

The institution is not required to provisionally credit a consumer's account to extend the time period for an investigation to 45 days if the institution requires but does not receive written confirmation within 10 business days of an oral notice of error or the alleged error involves an account that is subject to Regulation T, concerning securities credit by brokers and dealers.²⁸

90 Calendar Days Exception: The 45-day period can be extended to 90 days from the receipt of a notice if the conditions previously discussed for extending the time period to 45 calendar days are satisfied²⁹ and the error:

- involved an EFT that was not initiated within any state, territory, or U.S. possession; the District of Columbia; the Commonwealth of Puerto Rico; or any political subdivision (i.e., a foreign-initiated EFT);
- resulted from a point-of-sale debit card transaction; or
- occurred within 30 calendar days after the first deposit into the account.

REQUIREMENTS AFTER THE INVESTIGATION

After completing its investigation, a financial institution must:

- correct an error within one business day after determining that an error has occurred; and
- report the results of its investigation to the consumer (either orally or in writing,³⁰ unless the institution concludes that no error or a different error occurred, in which case the results must be in writing)³¹ within three business days after completing its investigation.³²

PROCEDURES IF NO ERROR OR DIFFERENT ERROR OCCURRED

If a financial institution concludes that either no error or a different error than the one alleged occurred, the institution must:

- include in its report of the results of the investigation a written explanation of the findings and a disclosure of the consumer's right to request the documents upon which the institution relied; and
- upon debiting a provisionally credited amount:
 - notify the consumer of the date and amount of the debit; and
 - notify the consumer that the institution will honor checks (or similar instruments payable to third parties) and preauthorized transfers from the consumer's account — without charging overdraft fees — for five business days after the notification, provided that the items honored would have been paid if the institution had not debited the provisionally credited funds.³³

If the consumer reasserts the error and the institution completed the initial investigation in compliance with the regulation, the institution has no further responsibilities to the consumer, except when a consumer asserts an error after receiving documentation requested under §1005.11(a)(1)(vii). See 12 C.F.R. §1005.11(e).

CONCLUSION

Financial institutions should review and test their policies and procedures regarding error resolution investigations to ensure that they comply with the requirements of the EFTA and Regulation E. The table on page 5 summarizes these requirements. Specific issues should be raised with your primary regulator. ■

EFT Errors Overview

Error Resolution Coverage	• Unauthorized EFT • Incorrect EFT • EFT omitted from the periodic statement • Computational error for EFT • Receipt for an incorrect amount of money from an electronic terminal • EFT not identified per §1005.9 or §1005.10(a) • Request for documentation under §1005.9 or §1005.10(a) or for information concerning an EFT
Consumer Obligations When Submitting Error Notice	• Oral or written notice must be received by the institution within 60 days after the institution sends the periodic statement reflecting the disputed transactions (can be extended for extenuating circumstances) • Notice must enable the institution to identify the consumer's name and account number • Notice must indicate why the consumer believes an error exists and include information about the error
Institution Obligations After Receiving an Error Notice	• Promptly investigate the oral or written allegation of the error • Complete its investigation within the time limits as specified in Regulation E • Correct the error within one business day after determining that an error has occurred • Report the results of its investigation within three business days after completing its investigation

ENDNOTES*

¹ Kenneth Benton and Robert Sheerr, "Error Resolution Procedures and Consumer Liability Limits for Unauthorized Electronic Fund Transfers," Consumer Compliance Outlook (Fourth Quarter 2012).

² 81 FR 83934 (November 22, 2016). In 2018, the Consumer Financial Protection Bureau amended the rule to change the effective date, modify the error resolution and consumer liability provisions, and make other changes. 83 FR 6364 (February 13, 2018). CCO previously discussed these requirements. See Scott Sonbuchner, "Error Resolution and Liability Limits for Prepaid Accounts and Foreign Remittance Transfers," Consumer Compliance Outlook (Second Issue 2021).

³ 15 U.S.C. §1693 et seq.

⁴ 15 U.S.C. §1693(b).

⁵ 12 C.F.R. §1005.15.

⁶ Prepaid accounts are addressed in 12 C.F.R. §1005.18, including modified rules in 12 C.F.R. §1005.18(e) for error resolution and liability.

⁷ Regulation E "applies to any electronic fund transfer that authorizes a financial institution to debit or credit a consumer's account." 12 C.F.R. §1005.3. See also 12 C.F.R. §1005.2(b)(3) (scope of Regulation E, including prepaid accounts, such as payroll cards and government benefit accounts), §1005.3 (overall coverage), §1005.20 (gift cards), and §1005.30–1005.36 (remittance transfers).

⁸ " 'Financial institution' means a bank, savings association, credit

union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services," other than auto dealers excluded from coverage of this part by §1029 of the Dodd–Frank Act. 12 C.F.R. §1005.2(i).

⁹ For example, the consumer withdraws \$100 but the terminal dispenses only \$20.

¹⁰ 12 C.F.R. §1005.11(a)(2).

¹¹ Comment 11(a)-4.

¹² When a notice of error is based on documentation or clarification that the consumer requested under §1005.11(a)(1)(vii), the notice is timely if the institution receives it no later than 60 days after the bank transmits the requested documentation. 12 C.F.R. §1005.11(b)(3).

¹³ Comment 11(b)(1)-1.

¹⁴ 12 C.F.R. §1005.11(b)(1). However, the consumer is not required to allege any specific error if the consumer requests documentation or clarification pursuant to 12 C.F.R. §1005.11(a)(1)(vii) to determine if an error occurred. 12 C.F.R. §1005.11(b)(1)(iii).

¹⁵ 12 C.F.R. §1005.11(b)(2).

¹⁶ Comment 11(b)(1)-5.

¹⁷ Comments 11(b)(1)-2 and 11(c)-2.

¹⁸ Comments 11(b)(1)-2 and 11(c)-2. See also CFPB EFTA Error Resolution FAQ 4.

ENDNOTES*

¹⁹ See EFTA §909(b) (codified at 15 U.S.C. §1693g(b)).

²⁰ 71 FR 1638, 1654 (January 10, 2006).

²¹ Comment 11(c)-4.

²² 12 C.F.R. §1005.11(c)(4).

²³ Comment 11(c)(4)-5.

²⁴ Comment 11(c)(4)-5.

²⁵ 12 C.F.R. §1005.11(c)(2).

²⁶ 12 C.F.R. §1005.11(c)(3)(i).

²⁷ 12 C.F.R. §1005.11(c)(2).

²⁸ 12 C.F.R. §1005.11(c)(2)(i); see also 12 C.F.R. Part 220 (Securities Credit by Brokers and Dealers).

²⁹ 12 C.F.R. §1005.11(c)(3)(ii).

³⁰ 12 C.F.R. §1005.11(c)(1); Comment 11(c)-1. Comment 11(c)-5 states that an institution may include the notice of correction on the periodic statement that is mailed or delivered within the time limits of 10 or 45 business days and clearly identifies the correction on the consumer's account.

³¹ Comment 11(d)(1)-1.

³² The three-day requirement applies to both 10-day and 45-day investigations. See 12 C.F.R. §1005.11(c)(1) and (c)(2)(iv), respectively.

³³ 12 C.F.R. §1005.11(d).

* Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

CONSUMER LIABILITY FOR UNAUTHORIZED TRANSACTIONS UNDER THE ELECTRONIC FUND TRANSFER ACT AND REGULATION E

BY KENNETH BENTON, PRINCIPAL CONSUMER REGULATIONS SPECIALIST, FEDERAL RESERVE BANK OF PHILADELPHIA

Editor's Note: *Consumer Compliance Outlook (CCO)* is updating a 2012 article reviewing the procedures financial institutions must follow under the Electronic Fund Transfer Act (EFTA) and Regulation E when consumers allege an error in an electronic fund transfer (EFT) to reflect regulatory changes that have occurred since it was published.¹

Part 1 of this two-part series discussed error resolution procedures under the EFTA and Regulation E. This second part discusses a consumer's potential liability when an institution investigates an error involving an unauthorized EFT and confirms that it was unauthorized.

CONSUMER LIABILITY FOR UNAUTHORIZED EFT: 12 C.F.R. §1005.6

When an institution receives notice from a consumer of an unauthorized EFT, and the institution confirms this after completing an investigation (as discussed in the companion article on error resolution procedures), the consumer's financial responsibility for the unauthorized EFTs is limited to the amounts described in §1005.6, which this article reviews in detail.

Conditions for Liability

The regulation does not permit an institution to impose liability on a consumer for an unauthorized transaction unless the institution previously provided the consumer with three disclosures required under §1005.7(b): a summary of the consumer's liability for unauthorized transactions, the telephone number and address of the person or office to be notified of an unauthorized EFT, and the financial institution's business days.

In addition, if the unauthorized transaction involved an *access device*, which the regulation defines as a "card, code, or other means of access to a consumer's account, that can be used by the consumer to initiate electronic fund transfers,"² it must be an *accepted* access device and the financial institution must have provided a means to identify the consumer to whom it was issued.³ An access device becomes an accepted access device when the consumer:

- requests and receives, or signs, or uses the device to transfer money between accounts or to obtain money, property, or services;

- requests the access device be validated without solicitation; or
- receives a renewal of, or substitute for, an existing accepted access device from the financial institution that issued the original access device or that institution's successor.⁴

The regulation and commentary explain that when determining a consumer's liability under §1005.6, banks cannot:

- use the consumer's negligence (for example, writing the PIN on a debit card) as a reason for imposing greater liability than allowed under the regulation;⁵
- impose greater liability on the consumer by agreement for unauthorized transfers than permitted under the regulation;⁶ or
- apply greater liability under the regulation when state law or an agreement with the consumer imposes lesser liability.⁷

In addition, the EFTA prohibits a financial institution from waiving a consumer's rights under the EFTA, including the right to file an action.⁸

Notice Requirements

The extent of a consumer's liability for an unauthorized EFT depends upon whether an access device is involved and when the consumer notifies its financial institution about the theft or loss of the device or about the unauthorized EFT. The consumer's notice is effective "when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information."⁹ Consumers may give notice in person, by phone, or in writing.¹⁰ Written notice is effective when the consumer mails the notice or delivers it by other usual means.¹¹

Other considerations regarding notification:

Notice by Third Party: For purposes of the limitations on liability under §1005.6, notice provided by a third party on the consumer's behalf is valid.¹² A financial institution may require "appropriate documentation" from the third party to ensure that the person is acting on the consumer's behalf.

Constructive Notice: An institution is deemed to have constructive notice, regardless of when the consumer provides actual notice, "when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized [EFT] to or from the consumer's account has been or may be made."¹³

Extension for Extenuating Circumstances: A financial institution must extend the time limits in 12 C.F.R. §1005.6(b) if the consumer failed to notify the institution because of "extenuating circumstances."¹⁴ When this occurs, the institution must extend the limits to "a reasonable period of time." Comment 6(b)(4)-1 lists hospitalization and extended travel as examples of extenuating circumstances under §1005.6(b)(4).

Liability for Unauthorized EFTs Involving an Access Device

Regulation E establishes three tiers of liability for unauthorized EFTs involving an access device. The applicable tier depends on when the consumer learned of the loss or theft of an access device, when the financial institution received notice, and when the financial institution transmitted the periodic statement showing the first unauthorized transaction to the consumer.

First Tier Liability (\$50 Maximum): §1005.6(b)(1). If the consumer notifies the financial institution within two business days¹⁵ after learning the access device was lost or stolen, the financial institution may hold the consumer liable only for the lesser of (a) \$50 or (b) the amount of the unauthorized EFTs that happened before the institution was notified.¹⁶

First Tier Liability: Example 1	
Monday	Consumer's debit card is stolen
Wednesday	Consumer learns of the theft
Thursday	Unauthorized EFT of \$100 using debit card
Friday	Consumer notifies the financial institution of the theft
The financial institution may not hold the consumer liable for more than \$50 of the \$100 transfer because the consumer provided notice within two business days of learning the access device was lost or stolen.	

First Tier Liability: Example 2

Monday	Consumer's debit card is stolen
Tuesday	Unauthorized EFT of \$35 using debit card
Wednesday	Consumer learns of the theft
Friday	Consumer notifies the financial institution of the theft
The financial institution may hold the consumer liable for the \$35 transfer because §1005.6(b)(1) specifies a consumer may be liable for up to \$50 of an unauthorized EFT when notice is provided within two business days of learning of the loss or theft.	

Second Tier Liability (\$500 Maximum): §1005.6(b)(2). If a consumer fails to notify the financial institution within two business days after learning that the access device was lost or stolen but notifies the institution of the loss or theft within 60 days of the financial institution's transmittal of the statement containing the error, the institution may hold the consumer liable for the lesser of (a) \$500 or (b) the sum of:

- (i) the consumer's first tier liability (i.e., the lesser of \$50 or the amount of unauthorized EFTs that occurred before the end of the second business day

after the consumer learns of the loss or theft); and

- (ii) the amount of the unauthorized EFTs that occurred after the end of the second business day after the consumer learns of the loss or theft and before the institution was notified, provided that the institution establishes that the unauthorized EFTs would not have occurred had the consumer provided notice within two business days after learning of the loss or theft.¹⁷

Second Tier Liability: Example 1¹⁸

Monday	Consumer's debit card is stolen and consumer learns of the theft
Tuesday	Unauthorized EFT of \$100 using debit card
Thursday	Unauthorized EFT of \$600 using debit card
Friday	Consumer notifies the financial institution of theft; the bank's systems are set up to immediately freeze an account after the notice of an unauthorized EFT. If the consumer had provided notice on Wednesday, the \$600 transfer would not have occurred.
The financial institution may hold the consumer liable for \$500, calculated as follows: • \$50 of the \$100 transfer, plus • \$450 of the \$600 transfer.	

Second Tier Liability: Example 2¹⁹

Monday	Consumer's debit card is stolen and consumer learns of the theft
Tuesday	Unauthorized EFT of \$600 using debit card
Thursday	Unauthorized EFT of \$100 using debit card
Friday	Consumer notifies the financial institution of the theft; the bank's systems are set up to immediately freeze an account after the notice of an unauthorized EFT. If the consumer had provided notice on Wednesday, the \$100 transfer would not have occurred.
The financial institution may hold the consumer liable for only \$150, calculated as follows: • \$50 of the \$600 transfer, plus • Entire \$100 transfer.	

Third Tier Liability (Unlimited): §1005.6(b)(3). If the consumer fails to notify the financial institution of the unauthorized EFT within 60 days after the financial institution transmits a periodic statement to the consumer showing the first unauthorized EFT, the financial institution may impose liability on the consumer up to the total amount of all unauthorized EFTs occurring more than 60 calendar days after transmitting the statement and before notice to the

financial institution, provided that the institution establishes that the unauthorized EFTs would not have occurred had the consumer notified the institution within the 60-day period. For unauthorized transactions that occurred *before* this period, the consumer is liable only to the extent that the banks could impose first and second tier liability under §1005.6(b)(1) and §1005.6(b)(1)(2), respectively.

Third Tier Liability: Example ²⁰	
January 1	Consumer’s debit card is stolen and consumer learns of the theft
January 2	Unauthorized EFT of \$100 using debit card
January 6	Unauthorized EFT of \$600 using debit card
January 30	Periodic statement is transmitted that showed unauthorized EFTs of \$100 and \$600
April 10	Unauthorized EFT of \$400 using debit card
April 11	Consumer notifies the financial institution of the theft (after 60 days of the transmittal of the periodic statement with the unauthorized transactions)
The financial institution may hold the consumer liable for \$900, calculated as follows: • \$50 of the \$100 transfer, plus • \$450 of the \$600 transfer, plus • \$400 of the \$400 transfer.	

Unauthorized EFTs Not Involving an Access Device

The consumer liability rules are slightly different when an unauthorized EFT does not involve an access device. Most importantly, the first two tiers of liability do *not* apply; that is, the institution may not hold a consumer liable for *any* portion of any unauthorized EFT not involving an access device that occurred on or before the 60th calendar day after the institution’s transmittal of the periodic statement showing

the first unauthorized EFT.²¹ Instead, an institution may *only* hold the consumer fully liable for transactions that occurred more than 60 calendar days after the periodic statement was transmitted showing the first unauthorized EFT and before the consumer provides notice to the financial institution. But the institution must also establish that the unauthorized EFTs would not have occurred had the consumer notified the institution within the 60-day period.

Liability for Unauthorized EFTs Not Involving an Access Device: Example ²²	
March 15	Consumer’s account is electronically debited without authorization for \$200
April 2	Financial institution transmits the periodic statement containing an unauthorized EFT
June 2	Unauthorized EFT of \$400 (61 days after periodic statement transmittal)
June 3	Consumer notifies the financial institution
The financial institution may hold the consumer liable for only \$400 of the total \$600 in transfers, calculated as follows: • \$0 of the \$200 transfer, and • \$400 of the \$400 transfer.	

The interagency examination procedures for Regulation E include a summary of the circumstances in which the

consumer may be liable for unauthorized EFTs (reproduced in the table below).²³

Summary of Consumer Liability for Unauthorized EFTs		
Event	Timing of Consumer Notice to Financial Institution	Maximum Liability
Loss or theft of access device	Within two business days after learning of loss or theft	Lesser of \$50 or the total amount of unauthorized transfers
	More than two business days after learning of loss or theft up to 60 calendar days after transmittal of statement showing first unauthorized transfer made with access device	Lesser of \$500 or the sum of: 1. \$50 or total amount of unauthorized transfers occurring in the first two business days, whichever is less, and 2. The amount of unauthorized transfers occurring after two business days and before notice to financial institution
	More than 60 calendar days after transmittal of statement showing first unauthorized transfer made with access device	For transfers occurring within the 60-day period, the lesser of \$500 or the sum of: 1. Lesser of \$50 or amount of unauthorized transfers in the first two business days, whichever is less, and 2. The amount of unauthorized transfers occurring after two business days For transfers occurring after the 60-day period, unlimited liability (until financial institution is notified)
Unauthorized transfer(s) not involving loss or theft of access device	Within 60 calendar days after transmittal of periodic statement on which unauthorized transfer first appears	No liability
	More than 60 calendar days after transmittal of periodic statement on which unauthorized transfer first appears	Unlimited liability for unauthorized transfers occurring 60 calendar days after periodic statement and before notice to financial institution

CONCLUSION

Financial institutions should review and test their policies and procedures regarding consumer liability for unauthorized

transactions to ensure they comply with requirements of the EFTA and Regulation E. Specific issues should be raised with your primary regulator. ■

ENDNOTES*

- ¹ Kenneth Benton and Robert Sheerr, “Error Resolution Procedures and Consumer Liability Limits for Unauthorized Electronic Fund Transfers,” *Consumer Compliance Outlook* (Fourth Quarter 2012).
- ² 12 C.F.R. § 1005.2(a)(1).
- ³ 12 C.F.R. § 1005.6(a).
- ⁴ 12 C.F.R. § 1005.2(a)(2).
- ⁵ Comment 6(b)-2.
- ⁶ Comment 6(b)-3.
- ⁷ 12 C.F.R. § 1005.6(b)(6).
- ⁸ 15 U.S.C. § 1693l.
- ⁹ 12 C.F.R. § 1005.6(b)(5)(i).
- ¹⁰ 12 C.F.R. § 1005.6(b)(5)(ii).
- ¹¹ 12 C.F.R. § 1005.6(b)(5)(iii).
- ¹² Comment 6(b)(5)-2.
- ¹³ 12 C.F.R. § 1005.6(b)(5)(iii).
- ¹⁴ 12 C.F.R. § 1005.6(b)(4) requires that, if the consumer experienced extenuating circumstances, the time period for providing notice is extended by a “reasonable period.”
- ¹⁵ 12 C.F.R. § 1005.6(b)(1). The commentary expands on this: “The two business day period does not include the day the consumer learns of the loss or theft or any day that is not a business day. The rule is calculated based on two 24-hour periods, without regard to the financial institution’s business hours or the time of day that the consumer learns of the loss or theft. For example, a consumer learns of the loss or theft at 6 p.m. Friday. Assuming that Saturday is a business day and Sunday is not, the two business day period begins on Saturday and expires at 11:59 p.m. on Monday, not at the end of the financial institution’s business day on Monday.” Comment 6(b)(1)-3.
- ¹⁶ Comment 6(b)(1)-1. The payment card networks, such as MasterCard, Visa, and Discover, typically provide in their agreement with participating merchants that the consumer generally has zero liability for unauthorized debit card transactions, subject to specified exclusions. Under § 1005.6(b)(6), if the consumer’s account agreement with the institution incorporates the payment card network liability limits, the institution could not impose liability greater than those limits.
- ¹⁷ 12 C.F.R. § 1005.6(b)(2).
- ¹⁸ Comment 6(b)(2)-1.
- ¹⁹ Comment 6(b)(2)-1.
- ²⁰ 12 C.F.R. § 1005.6(b)(3); Comment 6(b)(3)-1.
- ²¹ Comment 6(b)(3)-2.
- ²² Comment 6(b)(3)-2.
- ²³ Federal Reserve Consumer Affairs Letter 19-6, “Revised Interagency Examination Procedures for Regulation E,” (April 9, 2019). Revised Interagency Examination Procedures for Regulation E (at pp. 25–26).

* Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

FEDERAL RESERVE SYSTEM

COMMUNITY BANKING CONNECTIONS[®]

A SUPERVISION AND REGULATION RESOURCE

Community Banking Connections is the Federal Reserve System’s online resource that provides perspectives from bank examiners and Federal Reserve staff, addresses challenges and concerns facing community banks as well as provides resources to assist bankers.

Articles released over the past year provided insights on emerging issues from discount window borrowing to strategic planning.

Subscribe
Here



communitybankingconnections.org

ERROR RESOLUTION UNDER REGULATION E: EXAMINER INSIGHTS AND COMMON VIOLATIONS

BY SCOTT SONBUCHNER, EXAMINER, FEDERAL RESERVE BANK OF MINNEAPOLIS

This special issue of *Consumer Compliance Outlook* reviews error resolution requirements and consumers' liability for unauthorized electronic fund transfers (EFTs). This article discusses common violations Federal Reserve examiners have observed and the ways institutions can enhance their compliance management programs related to EFT errors.

NOT APPLYING LIABILITY LIMITS PROPERLY

When a consumer asserts an unauthorized transaction that occurred more than 60 days after the institution transmitted the periodic statement listing the disputed transaction, the institution is not required to follow the error resolution requirements of 12 C.F.R. §1005.11.¹ Examiners have found that some institutions mistakenly believe this timing requirement for error notices also applies to the limits on a consumer's liability for unauthorized transactions. However, the Official Staff Commentary for Regulation E clarifies that while a consumer has unlimited liability for transactions occurring after the 60-day period, the liability limits under §1005.6 still apply for transactions that occurred *prior to the 61st day*.²

As an example, consider this scenario. A consumer loses his card on January 1, 2025, and notices it is missing the same day. On January 2, 2025, \$400 of unauthorized transactions are made, and on January 6, 2025, \$600 of unauthorized transactions are made. The institution includes these transactions on the periodic statement it transmits to the consumer on February 5, 2025. On April 10, 2025, an unauthorized transaction for \$800 is made. The consumer notifies the financial institution of the lost card on April 30, 2025 (more than 60 days after the periodic statement showing the unauthorized transactions on January 2 and 6 was transmitted). His total liability of \$1,300 is calculated as follows:

- \$50 for the \$400 in unauthorized transfers that occurred on January 2, 2025,
- \$450 of the \$600 transfer that occurred on January 6, 2025, and
- \$800 for the unauthorized transaction that occurred on April 10, 2025.³

The risk here is that staff fail to understand the liability rules that have been discussed for unauthorized transactions. An institution can mitigate this risk by ensuring that its EFT error resolution procedures and training include specific guidance for the added protections for consumers who

allege unauthorized transactions. These added protections can be especially important when determining the effect of a late notice of error and when documenting consumers' promptness in reporting the loss or theft of an access device (i.e., a card, code, or other means to initiate electronic fund transfers from a consumer's account).⁴

NOT PROMPTLY INITIATING AN INVESTIGATION

A financial institution must investigate alleged errors promptly after receiving an error notice containing the information set forth in Regulation E,⁵ whether the notice was written or oral.⁶ While an institution may request a written confirmation after receiving an oral notice of error, it still must promptly begin investigating after receiving the oral notice.⁷ Additionally, although an institution may require that notice be provided only to the telephone number or address disclosed by the institution, if the consumer attempts to provide notice in a different manner, the institution must maintain reasonable procedures to refer the consumer to the specific telephone number or address required.⁸

An institution does not comply with the prompt investigation requirement if it requires, as a condition for starting the investigation, that consumers provide information not specified in the regulation. Common examples of requests that may not be used as a condition to begin the investigation, because the regulation does not require such information to be part of a consumer's error notice, include:

- asking a consumer to visit a branch to complete an error notice,
- requesting the consumer first tries to resolve the dispute with the merchant,
- requiring the consumer to submit a notarized affidavit, or
- indicating the consumer must file a police report.⁹

To help manage this risk, compliance officers can review error resolution procedures for any steps that may delay an investigation and confirm they are consistent with the regulatory requirement for a prompt investigation. Additionally, compliance officers can review the procedures for receiving consumer disputes from different channels to ensure disputes are routed to the correct point of contact. This could include tellers, receptionists receiving incoming calls, and email inboxes for consumer feedback.

NOT PROVIDING PROVISIONAL CREDIT

An institution choosing to extend an error investigation period beyond the time frame of 10 business days (or 20 days for new accounts) generally must provide provisional credit within 10 or 20 days, provided an exception does not apply.¹⁰

Examiners have seen instances in which the institution has taken more than 10 business days to investigate the error when an exception to providing provisional credit does not apply but fails to provide provisional credit or does not provide it in a timely manner. In some cases, the provisional credit covers the alleged error but fails to include interest when an interest-bearing account is involved. Provisional credit should include both the amount of the alleged error and interest, whenever applicable.¹¹

An institution can mitigate this risk by reviewing error resolution procedures, including provisional credit requirements, to confirm they align with Regulation E and by conducting training. Compliance officers may also benefit from reviewing error resolution logs for any extended investigations in which the bank did not provide provisional credit. For extended investigations in which the bank did not provide provisional credit, the institution can confirm whether the circumstances fall within the regulation's provisional credit exceptions, such as when the institution requires, but does not receive, written confirmation of an error.

NOT CONDUCTING A REASONABLE INVESTIGATION

A financial institution cannot deny a consumer's claim of an error without conducting a reasonable investigation. However, a financial institution may forgo the investigation if it corrects the error as alleged by the consumer. A reasonable investigation includes reviewing relevant information within the institution's records. An article on page 1 of this issue on Regulation E's resolution procedures discusses the reasonable investigation requirement in greater detail.

When the alleged error is an unauthorized EFT, the Electronic Fund Transfer Act (EFTA) places the burden of proof on the financial institution to establish that the transaction was authorized. Therefore, if the institution cannot establish that the disputed EFT transaction was authorized, the institution must credit the consumer's account.¹²

To mitigate this risk, compliance departments can conduct transaction testing on previously denied error notices. For each previously denied allegation within the selected sample, the institution can confirm that employees reviewed all relevant information within the institution's records and that the findings of the investigation met the institution's burden of proof to establish that an error did not occur. If the transaction

testing revealed the investigation was not adhering to regulatory requirements, the staff handling the investigations can receive additional training on this issue.

NOT COMPLYING WITH REQUIREMENTS FOR DENYING CLAIMS

A financial institution is required to follow specific regulatory requirements if it determines an error has not occurred or has occurred in a manner or amount different from what the consumer described. Within three business days after completing its investigation, the institution must report its results to the consumer. This explanation of findings must be in writing and disclose the consumer's right to request the documents used to make the denial. Upon a consumer's request, an institution must provide the documents.¹³ Regulators have seen institutions fail to meet these requirements.

The institution must follow one of two options to debit a previously provided provisional credit. Both options require the financial institution to honor checks and preauthorized transfers from the consumer's account (without a charge to the consumer for overdrafts that would have been paid had the provisional credit not been debited) for five business days. Under the option in §1005.11(d)(1)(i), the institution debits the amount first and then provides the consumer notice, which includes a statement that certain items will be honored for five business days after the notification. Under the second option described in Comment 11(d)(1)(ii)-1, the institution provides the notice first, specifies the calendar date on which debiting will occur, and then debits the amount five business days later. This option may be simpler for the institution but also gives the consumer more freedom with the provisional credit during the five days prior to the debit.

Regulators have seen issues when an institution's notice to consumers does not align with its actual practice for debiting provisional credit. This can happen because template language is not accurate, or employees are not knowledgeable about bank processes. For example, if the provisional credit is debited immediately upon notice, an institution must notify the consumer that third-party payments and preauthorized transfers will be honored for five days. But if an institution uses the alternative option from the Official Staff Commentary to Regulation E, the provisional credit cannot be debited until five business days after the notice is provided.

To mitigate these risks, compliance officers can review bank procedures, interview appropriate staff, and review template letters. Procedures and staff practices need to comply with Regulation E and be consistent with the template letters that employees send to consumers. In cases in which misalignment among written procedures, employee practices, and templates exists, consider retraining employees to ensure they follow the bank's practices correctly.

NOT COMPLYING WITH REQUIREMENTS FOR CORRECTING ERRORS

If, after completing an investigation, an institution determines an error occurred, it must correct the error within one business day and report the results to the consumer within three business days, subject to the liability provisions of §§1005.6(a) and (b). This correction should include, as applicable, a credit for interest and a refund of fees charged by the institution. While reviewing practices for correcting alleged errors, regulators have found institutions failing to provide timely corrections of errors and notices to consumers. Examiners have also observed some institutions failing to include lost interest and fees caused by the error (e.g., an error resulted in an overdraft fee) in monetary adjustments provided to consumers.

An institution's compliance officers can mitigate timing and consumer notification issues by properly documenting requirements and training employees. However, in some cases, determining the full amount of an error may be complicated. For instance, employees may need to examine the account and look at transactions that occurred around the same time as the error or to postdate the credit so the account can accrue the interest. Depending on how the bank's systems and accounts are configured, reducing risk may involve more detailed discussions with employees who have a comprehensive understanding of the bank's deposit account systems.

NOT COMPLYING WITH REQUIREMENTS AFTER INVESTIGATION IS FINAL

Once a financial institution has fully complied with the error resolution requirements in §1005.11, a consumer may not reassert the same error. But this finality can also present a challenge to institutions because once a financial institution provides notice that a provisional credit has been made final,¹⁴ the financial institution generally cannot reopen the

investigation or reverse the credit. For example, if an institution provisionally credits a consumer's account while investigating an error, determines an error occurred, and notifies a consumer that the provisional credit is final, but later learns the merchant refunded the consumer or that the transaction was authorized, the institution cannot reverse the credit.

An exception applies for foreign remittance transfers where the consumer alleges the same error to multiple parties. For example, suppose a consumer reports to a remittance transfer provider that it committed an error of \$100 in executing a remittance transfer. The provider refunds the \$100 after investigating and determining an error occurred. If the consumer subsequently alleges the same error with the institution holding the account, and that institution refunds the \$100 after investigating but later learns of the prior refund from the remittance transfer provider for the same error, the institution holding the account may reverse the amount it previously credited to the consumer's account.¹⁵

Steps to help mitigate this risk include educating the appropriate staff about the consumer protections under Regulation E for errors. Depending on a bank's culture, training covering Regulation E can benefit employees handling deposit operations as much as it benefits compliance staff. Having employees in different areas of the organization attend training together can help ensure that all understand when the bank's discretion ends and its legal obligations begin.

CONCLUSION

This article reviewed violations examiners have observed of Regulation E's error resolution requirements and discussed sound practices to facilitate compliance. Specific issues and questions should be raised with your primary regulator. ■

ENDNOTES*

¹ See 12 C.F.R. §1005.11(b)(1). Alternative time limits may apply to government benefit cards and prepaid accounts. See §1005.15(e)(3)–(4) (benefit cards) and §1005.18(e) (prepaid cards).

² See Comment 11(b)(1)-7.

³ See 12 C.F.R. §1005.6(b)(2): "If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$500 or the sum of ... \$50 or the amount of unauthorized transfers that occur within the two business days, whichever is less."

⁴ 12 C.F.R. §1005.2(a)(1).

⁵ See 12 C.F.R. §1005.11(b)(1).

⁶ See 12 C.F.R. §1005.11(c)(1).

⁷ See Comment 11(c)-2.

⁸ See Comment 11(b)(1)-6.

⁹ See Comments 11(b)(1)-2 and 11(c)-2.

¹⁰ An exception applies under §1005.11(b)(2) if the institution requires written confirmation of an error within 10 days of an oral notice but does not receive it. In that case, the institution may extend the investigation period without providing

ENDNOTES*

- provisional credit. Comment 11(b)(2)-1. The regulation requires that the consumer be notified of the written confirmation requirement when the oral notice of an error is made and the institution must provide the address to send the confirmation.

¹¹ See Comment 11(c)-6.

¹² See EFTA Section 909(b) (codified at 15 U.S.C. §1693.g(b). See also 83 FR 6364, 6382 (February 13, 2018): “Under EFTA section 909(b), the burden of proof is on the financial
- institution to show that an alleged error was in fact an authorized transaction; *if the financial institution cannot establish proof of valid authorization, the financial institution must credit the consumer’s account.*” (Emphasis added.)

¹³ 12 C.F.R. §1005.11(d); Comment 11(d)-1.

¹⁴ See 12 C.F.R. §1005.11(c)(2)(iv).

¹⁵ See Comment 33(f)-3.

* Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

CONTINUED FROM PAGE 1

THE ELECTRONIC FUND TRANSFER ACT, REGULATION E, AND INSTANT PAYMENT SERVICES

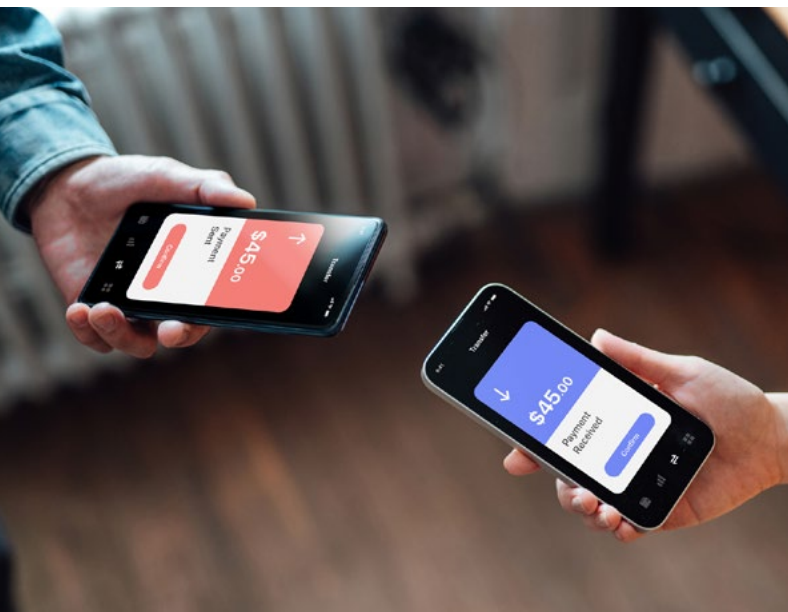
Instant Payment Services: RTP and FedNow Service

In 2017, TCH took the next step in providing faster payments when it introduced RTP, which provides instant, *credit* transfers⁶ 24 hours a day, 365 days a year for institutions participating in the RTP network and for transfers within the United States only. In 2023, the Federal Reserve launched its

FedNow Service, another instant payment service allowing consumers, businesses, and government to make instant credit payments to a business or consumer in the United States with an account at a financial institution participating in the FedNow Service.⁷ The table below compares the features of the two services.

Comparison of the FedNow Service and RTP		
	FedNow Service	RTP
Availability	24/7/365	24/7/365
Transaction Limit (as of September 2025)	\$10 million	\$10 million
Cycle Time	7 a.m.–7 p.m.	12:00 a.m.–12:00 p.m.
Ownership	Federal Reserve Banks	The Clearing House
Type of Instant Payments	Credit push only	Credit push only
Transaction Fee	.045¢	.045¢
Settlement Time	Instant	Instant
Revocability	Irrevocable	Irrevocable
Cross Border?	No	No
Messaging Standard	ISO 20022	ISO 20022
Number of participating institutions (as of September 2025)	1,477	1,056

Sources: Federal Reserve Bank Services, The Clearing House



LEGAL FRAMEWORK FOR INSTANT PAYMENTS: THE EFTA AND REGULATION E

Because RTP and the FedNow Service are relatively new payment rails, questions have arisen about how the Electronic Fund Transfer Act (EFTA) and Regulation E relate to these services when used for consumer transactions. We discuss the legal framework here.

EFTA/Regulation E

The rules for both the FedNow Service and the RTP service include specific references to the EFTA. That law and its implementing Regulation E (12 C.F.R. Part 1005) apply to “any electronic fund transfer that authorizes a financial institution to debit or credit a consumer’s account.”⁸ Regulation E defines *account* as “a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes.”⁹ The regulation further defines *electronic fund transfer* (EFT) as any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account. The regulation also provides examples of transfers that meet the definition of an EFT and examples of transfers that do not.¹⁰

FedNow Service

In June 2022, the Federal Reserve Board issued a final rule¹¹ to amend its Regulation J, 12 C.F.R. Part 210 (Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire) to add Subpart C,

“Funds Transfers Through the FedNow Service,” 12 C.F.R. §§210.40–47. This subpart specifies the terms and conditions under which Reserve Banks process electronic fund transfers with the FedNow Service and provides the legal framework for issues arising from use of the service. Under §210.40(b)(4) of Regulation J, Article 4A of the Uniform Commercial Code (UCC)¹² governs FedNow Service transactions, *except* when Article 4A is inconsistent with the EFTA, in which case “the [EFTA] shall prevail to the extent of the inconsistency.” The Official Staff Commentary for §40(b)(4) further clarifies this:

Under section 4A-108 [of the UCC], Article 4A does not apply to a funds transfer, any part of which is governed by the Electronic Fund Transfer Act (EFTA) (15 U.S.C. 1693 et seq.). A funds transfer from a consumer originator or a funds transfer to a consumer beneficiary could be carried out through the FedNow Service and could potentially be subject to the EFTA and Regulation E (12 CFR part 1005) implementing it. *If so, the funds transfer continues to also be governed by subpart C, except that, in the event of an inconsistency between the provisions of subpart C and the EFTA, the EFTA shall prevail to the extent of the inconsistency.* ... For example, a funds transfer may be initiated from a consumer’s account at a depository institution, and the depository institution may execute that payment order by sending a conforming payment order to a Reserve Bank through the FedNow Service. If that transfer is subject to the EFTA, then examples of how the provisions of subpart C may govern the transfer include, but are not limited to, the following:

(i) Where the consumer subsequently gives timely notice that the transfer was an unauthorized electronic fund transfer to its depository institution and exercises the right to obtain a refund under the EFTA, *the depository institution would be required to comply with the EFTA and the applicable provisions of the EFTA would govern the institution’s obligations to its customer, even if under subpart C the institution does not have a right to receive a refund or reverse the payment order sent to the Reserve Bank through the FedNow Service.*

(ii) Where the customer properly asserts an error under the EFTA with respect to the transfer and exercises the right to obtain a refund to correct the error under the EFTA, *the depository institution would be required to comply with the EFTA and the applicable provisions of the EFTA would govern the institution’s obligations to its customer, even if under subpart C the institution is obliged to pay its payment order sent to the Reserve Bank through the FedNow Service.*¹³ (Emphasis added)

The Board further addressed the application of the EFTA

and Regulation E to FedNow transactions in the preamble of the *Federal Register* notice of the 2022 final rule. Although Regulation J specifies that Article 4A generally governs the rights, obligations, and liabilities of participants in the FedNow Service, and Article 4A generally allows participants to vary their provisions by agreement of the affected parties, the Board noted in the preamble that “banks must nevertheless comply with requirements under other applicable law that, unlike UCC Article 4A, cannot be varied by agreement, such as applicable consumer protection requirements under the EFTA.”¹⁴

RTP

The RTP operating rules address the application of the EFTA and Regulation E to RTP transactions:

EFTA Consumer Payments. For an RTP Payment any part of which is subject to the EFTA, the rights and obligations of a Participant and a Consumer Customer shall be governed by:

a. *the EFTA and Regulation E, to the extent applicable to the transaction, and,*

b. to the extent consistent with EFTA and Regulation E as applicable to an RTP Payment, by these RTP Operating Rules, and the laws of the State of New York, excluding Article 4-A of the New York Uniform Commercial Code.¹⁵ (Emphasis added.)

CONCLUSION

Electronic payments have evolved from ACH transfers in the 1970s, which took several business days to settle, to the current availability of instant payment services. The instant payment rails benefit all stakeholders in the payment system. Although the rules of these instant payment services vary to a degree, to the extent that a fund transfer initiated to or from a consumer account using the FedNow Service or RTP is an EFT under Regulation E, that transfer would be subject to the EFTA and Regulation E. Specific questions should be addressed to your primary regulator. ■

ENDNOTES*

¹ See “Automated Clearing House Payments” on www.federalreservehistory.org. We have omitted a discussion of wire transfer services, such as FedWire and the Clearing House Interbank Payments System.

² See “Automated Clearinghouse Services” on www.federalreserve.gov.

³ See “Nacha Operating Rules” on www.nacha.org.

⁴ “Federal Reserve Announces Posting Rules for New Same-Day Automated Clearing House Service,” press release (June 21, 2010).

⁵ See “Same-Day ACH” on www.nacha.org.

⁶ A *credit transfer* refers to an electronic payment initiated by the *sender*. This contrasts with a debit transfer, in which a financial institution receives a request for a payment the recipient initiated.

⁷ See “About the FedNow Service” on www.frbsservices.org.

⁸ 12 C.F.R. §1005.3(a). See also 15 U.S.C. §1693a(2) (defining *account*), §1693a(7) (defining *electronic fund transfer*) and §1693a(9) (defining *financial institution*).

⁹ 12 C.F.R. §1005.2(b)(1).

¹⁰ 12 C.F.R. §1005.3(b).

¹¹ 87 FR 34350 (June 6, 2022).

¹² The Board included the text of Article 4A in Appendix A to Part 210 that applies to FedNow Service transactions. Because some states have slight variations in their versions of the UCC, it is important that financial institutions use this version. For example, the Uniform Law Commission amended Article 4A-108 in 2012 to address an amendment to the EFTA in §1073 of the Dodd–Frank Act to provide protections for consumer foreign remittance transfers. (The Consumer Financial Protection Bureau implemented the amendment in Subpart B of Regulation E, 12 C.F.R. §§1005.30–36.) Wyoming did not adopt this amendment. See Wyoming Statute §34-1-4.A-108. The Board’s version of Article 4A includes the amended §4A-108.

¹³ Comment 40-b.4 (Appendix A to Subpart C).

¹⁴ 87 FR 34351 (June 6, 2022).

¹⁵ RTP Operating Rules at p. 15 (June 16, 2025).

* Note: The links for the references listed in the Endnotes are available on the *Consumer Compliance Outlook* website at consumercomplianceoutlook.org.

REGULATORY CALENDAR

Rules Currently in Effect or Proposed

Final and proposed rules that have not been affected by the ongoing regulatory review

DATE†	REGULATION	REGULATORY CHANGE
10/01/25	Reg. Z	Agencies issue final rule on quality control standards for automated valuation models
08/26/25	CFPA §1024	Consumer Financial Protection Bureau (CFPB) issues proposed rule to adopt a standard for when to designate nonbank covered persons for Bureau supervision under §1024(a)(1)(c) of the Consumer Financial Protection Act (CFPA)
08/22/25	DFA §1033	CFPB issues advance notice of proposed rulemaking for reconsideration of open-banking rulemaking under §1033 of the Dodd–Frank Act (DFA)
08/15/25	n/a	CFPB releases its spring regulatory agenda
07/01/25	Reg. CC	Agencies implement inflation-adjusted dollar thresholds for Regulation CC funds availability
06/18/25	Reg B	CFPB issues interim final rule to extend compliance deadlines for §1071 of the DFA for small business loan data collection
06/03/25	FHA regulations	Rescission of Affirmative Fair Housing Marketing Regulations (24 CFR Part 108 and 24 CFR 200.600–200.640)
01/01/25	Reg. Z	Agencies announce dollar thresholds for smaller loan exemption from appraisal requirements for higher-priced mortgage loans
01/01/25	Regs. M and Z	Agencies adjust dollar thresholds for consumer credit and lease transactions
07/26/24	FHA, Regs. Z and B	Final Interagency Guidance on Reconsiderations of Value of Residential Real Estate Valuations
05/14/24	Reg. Z	CFPB issues final rule for credit card penalty fees
04/29/24	24 C.F.R. §100.500	Guidance on Application of the Fair Housing Act to the Advertising of Housing, Credit, and Other Real Estate-Related Transactions Through Digital Platforms
11/14/23	Reg. II	Federal Reserve issues proposal to lower the maximum interchange fee a large debit card issuer may charge
10/12/23	Reg. B	CFPB and Department of Justice issue Joint Statement on Fair Lending and Credit Opportunities for Noncitizen Borrowers Under the Equal Credit Opportunity Act

† Because proposed rules do not have an effective date, we have listed the *Federal Register* publication date.

REGULATORY CALENDAR

Rules Under Review

Prior proposed rules or final rules that were subsequently rescinded, stayed in litigation, or otherwise under review

DATE	REGULATION	REGULATORY CHANGE	STATUS
10/01/25	Regs. E and Z	CFPB issues final rule for overdraft fee for very large financial institutions	Repealed 05/08/25
05/12/25		CFPB rescinds 67 guidance documents	Rescinded
03/17/25	Reg. V	CFPB issues final rule to limit the use of medical debt in underwriting consumer credit	Stayed in litigation
01/17/25	12 U.S.C. §1033	CFPB issues final rule on personal financial data rights	Stayed in litigation
01/09/25	12 C.F.R. §1090.109	CFPB issues larger participant final rule for the general-use digital consumer payment applications market	Stayed in litigation
12/13/24	Reg. V	CFPB proposes defining data brokers as consumer reporting agencies subject to the Fair Credit Reporting Act	Withdrawn 05/15/25
07/30/24	Reg. Z	CFPB issues interpretive rule applying certain provisions of Regulation Z to Buy Now, Pay Later loans	Withdrawn 05/12/25
05/14/24	Reg. Z	CFPB issues final rule for credit card penalty fees	Vacated 04/14/25
02/01/24	Reg. BB	Agencies issue final rule to modernize their implementing regulations for the Community Reinvestment Act	Withdrawn 07/16/25
01/31/24	12 C.F.R. §1042.2	CFPB issues proposal to prohibit fees for instantaneously declined transactions	Withdrawn 01/14/25
10/30/23	n/a	Agencies issue principles for climate-related financial risk management for large financial institutions	OCC Withdrawal 03/31/25

HOW TO SUBSCRIBE TO *CONSUMER COMPLIANCE OUTLOOK* AND OUTLOOK LIVE

CCO and Outlook Live are complimentary Federal Reserve System outreach platforms. *CCO* is a quarterly newsletter focusing on federal consumer compliance topics, while Outlook Live is a webinar series focusing on consumer compliance topics.

To subscribe to *CCO* and Outlook Live, please visit consumercomplianceoutlook.org. There, you can choose to receive future editions of *CCO* in electronic or print format. If you provide your email address while subscribing, we will also notify you by email of upcoming Outlook Live webinars.

Suggestions, comments, and requests for back issues are welcome in writing, by telephone (215-574-6500), or by email (outlook@phil.frb.org). Please address all correspondence to:

Kenneth Benton, Editor
Consumer Compliance Outlook
Federal Reserve Bank of Philadelphia
SRC 7th Floor NE
Ten Independence Mall
Philadelphia, PA 19106

CALENDAR OF EVENTS

November 6–7, 2025 **New Perspectives on Consumer Behavior in Credit and Payments Markets Conference**
Federal Reserve Bank of Philadelphia
Philadelphia, PA

November 16–19, 2025 **CRA & Fair Lending Colloquium**
JW Marriott Los Angeles
Los Angeles, CA

Scan with your smartphone
or tablet to access *Consumer
Compliance Outlook* online.



consumercomplianceoutlook.org