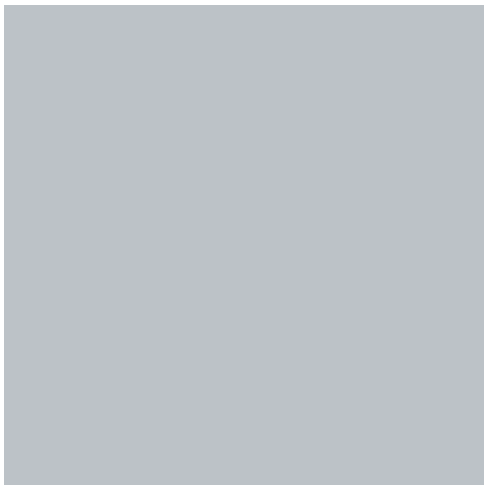
The Clearing House®

Error Resolution for P2P Payment Services: Beyond the CFPB FAQs

September 2022






Executive Summary

An Intermediated Transfer is a type of P2P transfer where funds are sent from a Sender to a Receiver through a Transfer Provider. The Sender is typically a consumer. In an Intermediated Transfer, the Transfer Provider executes the Sender's instruction to send funds to the Receiver via two separate transactions: a Funding Transaction and a Payment Transaction. As a result of these two distinct transactions, the Sender in an Intermediated Transfer has a relationship with two Financial Institutions: the Sender's Bank, which is the Financial Institution holding the Sender's deposit account used to fund the transfer, and the Transfer Provider, which is the Financial Institution providing the EFT service.

Both Financial Institutions involved in an Intermediated Transfer have error resolution obligations under the Electronic Fund Transfer Act and Regulation E, however, the scope of the obligations differ. As the Sender's Bank is only involved in the Funding Transaction, its error resolution obligations are limited to errors specific to the Funding Transaction. In contrast, the Transfer Provider is involved in the entire Intermediated Transfer and therefore it has error resolution obligations for the Intermediated Transfer regardless of whether the error relates to the Funding Transaction or the Payment Transaction.

As a result of the different scope of responsibility, the type of error asserted by the Sender matters in determining which Financial Institution has error resolution obligations. For example, if a Sender asserts to both Financial Institutions that an Intermediated Transfer is unauthorized, both Financial Institutions must investigate and resolve the error because the claim involves the Funding Transaction (except where the Transfer Provider is also a Service Provider, as discussed below). However, if a Sender asserts an Intermediated Transfer was delivered to the wrong person, only the Transfer Provider must investigate and resolve the error because the claim involves the Payment Transaction component of the Intermediated Transfer and is not specific to the Funding Transaction.

Moreover, even in connection with the Funding Transaction, the Sender's Bank is excused from the bulk of Regulation E's error resolution obligations when the Transfer Provider is also treated as a Service Provider. Under Regulation E, a Service Provider is a specific type of Financial Institution that issues an Access Device for an Account it does not hold and has no agreement regarding the Access Device with the Financial institution that holds the Account. A Transfer Provider is a Service Provider whenever the Funding Transaction involves an ACH debit from the Sender's Account. In such instances, the Transfer Provider has full error resolution obligations for the Intermediated Transfer and the Sender's Bank is exempt from the requirement to conduct its own error investigation or otherwise resolve the Sender's assertion of an error even for the Funding Transaction.

Table of Contents

Index of Defined Terms and Acronyms

I. Introduction

In 2021, the Consumer Financial Protection Bureau ("CFPB") issued Frequently Asked Questions regarding the Electronic Fund Transfer Act ("EFTA") and its implementing regulation, Regulation E, first on June 4, 2021, and then in an updated version on December 13, 2021 (collectively, "EFT FAQs"). The EFT FAQs address a number of topics, including error resolution, liability for unauthorized electronic fund transfers, and the application of Regulation E to consumer "person to person" ("P2P") payment services. Importantly, the EFT FAQs reiterate that both depository institutions and non-bank providers of P2P payment services ("P2P Providers") have error resolution obligations under Regulation E if they meet the definition of a "financial institution."

However, P2P payment services raise a number of issues under Regulation E that the EFT FAQs did not specifically address. For example, the CFPB did not clearly distinguish the different types of P2P payment services or directly address certain details about the various parties' Regulation E obligations related to Intermediated Transfers where a consumer ("Sender") instructs a Transfer Provider to send funds to another person ("Receiver") and the P2P transfer is funded by a debit to the Sender's account at a depository institution. As discussed further herein, such Intermediated Transfers involve two separate transactions to carry out the Sender's instruction and the Sender's depository institution has little, if any, information about the Intermediated Transfer being funded.

Given the nature of Intermediated Transfers, which involve more than one Financial Institution, there can be ambiguity about each Financial Institution's role and responsibility for investigating and resolving errors. As P2P payment services that use Intermediated Transfers grow in popularity, clarity regarding how this important consumer protection framework functions is critical for both the financial services industry and consumers.

I.A. Intermediated Transfers Covered in This Paper

The purpose of this paper is to describe the application of the Regulation E error resolution requirements to the Financial Institutions involved in an Intermediated Transfer: the P2P Provider that effectuates a P2P transfer as an Intermediated Transfer ("Transfer Provider") and the depository institution holding the Sender's Account that is used to fund an Intermediated Transfer ("Sender's Bank"). This paper focuses on each party's error resolution obligations when a Sender provides a notice of error involving an Intermediated Transfer.

Like other P2P transfers, Intermediated Transfers accomplish a desired transfer by acting on an instruction from the Sender to transfer funds to the Receiver. However, when a Sender instructs a Transfer Provider to pay the Receiver, the Transfer Provider executes that instruction via two distinguishable transactions: (1) a funding transaction in which funds are debited from the Sender's Account (as defined in Section III.A.2 below) at the Sender's Bank and delivered to the Transfer Provider or its agent ("Funding Transaction"),and (2) a payment transaction in which funds are delivered by the Transfer Provider to the Receiver's account held with the Transfer Provider or with another depository institution ("Payment Transaction"). Together, the Funding Transaction and the Payment Transaction constitute the "Intermediated Transfer." As both transactions must occur under the same instruction, the Sender must identify a Receiver as part of the transfer instruction to the Transfer Provider.

Many mobile or digital wallets allow consumers to both establish a Stored Balance (defined below) *and* engage in Intermediated Transfers. Such wallets are covered in this paper. As described more fully in Part II below, these wallets may allow consumers to fund Intermediated Transfers from a Funding Transaction or to initiate a "Split-Funded P2P Transfer" where a P2P transfer is funded in part by a Funding Transaction and in part by a Stored Balance. The portion of a Split-Funded P2P Transfer that is funded by a Funding Transaction is an Intermediated Transfer; the portion of a Split-Funded P2P Transfer that is funded by a Stored Balance is a "Stored Balance Transfer." However, as discussed below, P2P transfers fully funded by a Stored Balance are not Intermediated Transfers and are not the focus of this paper.

I.B. Other Digital Wallets and P2P Transfers Not Covered in This Paper

A mobile or digital wallet where the wallet merely serves as a pass-through mechanism for presenting the paying consumer's payment credentials to a seller for the purchase of goods or services does not involve an Intermediated Transfer. These types of mobile or digital wallets store payment

credentials, typically a debit[1] or credit card, on behalf of the paying consumer and allow the consumer to pay using a digital version of their payment credentials. The payment is processed by the seller in the same manner as if the physical card had been presented and funds move directly from the consumer to the seller in one transaction. As these wallets do not utilize Intermediated Transfers, they are outside the scope of this paper.

Some mobile or digital wallets allow consumers to store funds in the wallet ("Stored Balance") and use that Stored Balance to make P2P transfers. P2P transfers that are fully funded by a Stored Balance also do not involve Intermediated Transfers. These transfers do involve two transactions: one transaction where the consumer instructs the P2P Provider to load funds to the consumer's wallet from the consumer's bank account at their depository institution and a separate transaction where the consumer identifies a recipient and instructs the P2P Provider to send funds from the Stored Balance in the wallet to the identified recipient. However, they are not Intermediated Transfers because the consumer must provide separate instructions for each transaction and the transactions may bear no relation to each other. The consumer does not identify the recipient in connection with the first transaction (i.e., before loading the funds to the wallet) and the consumer may not have any intent to transfer the loaded funds to a third party at the time of the load transaction. Transactions to fund a Stored Balance in a mobile or digital wallet and transactions to make a P2P transfer funded entirely from a Stored Balance in a mobile or digital wallet are not the focus of this paper because they do not involve Intermediated Transfers.[2]

[1] As used in this paper, the term debit card includes a prepaid card.

[2] While these transactions are not addressed in this paper because they are not Intermediated Transfers, they are nevertheless subject to Regulation E, and the parties involved in these transactions must comply with Regulation E in connection with asserted errors to the extent such parties are Financial Institutions for the applicable part of the transaction.

II. Overview of the Transfer Provider Operating Models

Transfer Providers offering Intermediated Transfers typically operate through one of two models: a Prepaid Account model or a Staged Wallet model (or a combination of the two models). Under both models, the Funding Transaction in an Intermediated Transfer typically is accomplished through an ACH debit or a debit card transaction,[3] and the Payment Transaction typically is accomplished through a book-entry transfer on the ledger of the Transfer Provider, through an ACH credit, or through a push of funds over debit card rails.

II.A. Operating Models: Prepaid Account and Staged Wallet

II.A.1. Prepaid Account Model

Under the Prepaid Account model, the Sender establishes an Account (as defined in Section III.A.2 below) with the Transfer Provider ("Prepaid Account"). The Prepaid Account can be used to maintain a Stored Balance and the Prepaid Account's main function is to send funds via P2P transfers or pay sellers for goods or services. The Stored Balance may come from either funds loaded from the Sender's Bank or funds received from other Senders.

An Intermediated Transfer occurs when the Sender who has established a Prepaid Account instructs the Transfer Provider to transfer funds from the Sender's Account at the Sender's Bank to a Receiver. Although the Sender has established a Prepaid Account with the Transfer Provider, proceeds from the Funding Transaction in an Intermediated Transfer do not become part of the Stored Balance in the Prepaid Account. Instead, the funds typically are transitorily held in a money transfer account controlled by the Transfer Provider ("TP Account") only until those funds are transferred from the TP Account to the Receiver in the Payment Transaction. An Intermediated Transfer is funded wholly through the Funding Transaction. If a portion of the P2P transfer is funded by a Stored Balance in the Prepaid Account and in part through a Funding Transaction, it is a Split-Funded P2P Transfer.[4]

II.A.2. Staged Wallet Model

Under the Staged Wallet model, the Sender does not establish an Account (as defined in Section III.A.2 below) with the Transfer Provider and the Sender may not hold a Stored Balance with the Transfer Provider. Instead, the Sender establishes a profile (including a username and password) with the Transfer Provider, which can be used to facilitate Intermediated Transfers through the Transfer Provider's mobile application or website ("Wallet"). Funds from the Funding Transaction in an Intermediated Transfer involving the Staged Wallet model also typically are held transitorily in a TP Account before being pushed to the Receiver through the Payment Transaction.

All transfers using a Wallet must be Intermediated Transfers because there is no Prepaid Account or Stored Balance with the Transfer Provider. Each Intermediated Transfer is fully funded from a Funding Transaction and each Intermediated Transfer results in payment to the Receiver through a Payment Transaction.

II.B. Funding Transaction Methods

The Transfer Provider, through its relationship with a depository institution that participates in the ACH network or a card network, initiates a debit to the Sender's Account.

II.B.1. ACH Debit

The Transfer Provider, as an originator under the Nacha Rules governing the ACH network, uses the Sender's routing/transit number and bank account number to originate an ACH debit to the Sender's Account for credit to the TP Account.

[3] Credit cards also may be used to fund a Funding Transaction with some Transfer Providers, for a fee. Use of a credit card for the Funding Transaction would invoke consumer protections under the Truth in Lending Act and its implementing regulation, Regulation Z, and is beyond the substantive scope of this paper.

[4] Not all transfers a Sender makes involving a Transfer Provider that operates under a Prepaid Account model are part of an Intermediated Transfer. A transfer from the Sender's Account at the Sender's Bank to load funds to a Stored Balance is not an Intermediated Transfer because it does not involve a Payment Transaction. A transfer to a recipient funded entirely from a Stored Balance is not an Intermediated Transfer because these transfers involve separate instructions to load funds to the Prepaid Account and to send funds to the recipient.

II.B.2. Debit Card

The Transfer Provider, as a merchant participating in the payment card networks, uses information from the Sender's debit card to initiate a debit from the Sender's Account for credit to the TP Account.

II.C. Payment Transaction Methods

II.C.1. Book Entry

The Transfer Provider operating under a Prepaid Account model credits funds from the TP Account to the Receiver's Prepaid Account with the Transfer Provider.[5]

II.C.2. ACH Credit

The Transfer Provider, as an originator under the Nacha Rules, uses the Receiver's routing/transit number and bank account number to originate an ACH credit to the Receiver's bank account from the TP Account.

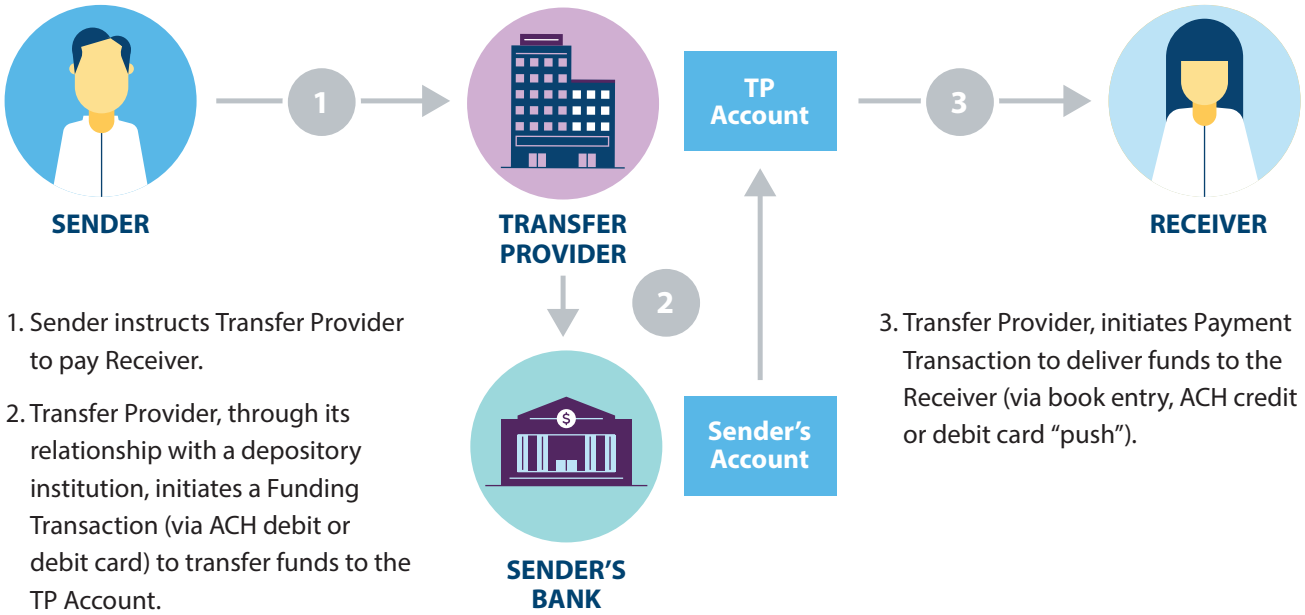
II.C.3. Debit Card

The Transfer Provider, as a merchant participating in the payment card networks, uses information from the Receiver's debit card to initiate a credit to the Receiver's bank account from the TP Account.

See an example illustration of an Intermediated Transfer on page 5. See example illustrations of a Split-Funded P2P Transfer and a Stored Balance Transfer in Appendix B on pages 32 and 33.

[5] The Receiver may also elect to withdraw funds from their Prepaid Account to their bank account via ACH, an RTP payment or a debit card "push" payment. The Receiver may also elect to send the funds to another recipient that participates in the Transfer Provider's service. This withdrawal or payment to another recipient occurs via a separate instruction after the completion of the Intermediated Transfer and is not part of the Payment Transaction.

Intermediated Transfer Example Illustration



1. Sender instructs Transfer Provider to pay Receiver.
2. Transfer Provider, through its relationship with a depository institution, initiates a Funding Transaction (via ACH debit or debit card) to transfer funds to the TP Account.
3. Transfer Provider, initiates Payment Transaction to deliver funds to the Receiver (via book entry, ACH credit or debit card "push").

Notes:

- For simplicity, the illustration does not reflect the Transfer Provider's bank, which at the Transfer Provider's direction would originate/transmit the Funding Transaction into the ACH network or card network. The same bank may also hold the TP Account for the Transfer Provider.
- The illustration does not distinguish between the Prepaid Account Model and the Staged Wallet Model as both support Intermediated Transfers.
  a. In the Prepaid Account Model, an Intermediated Transfer occurs when the Payment Transaction is funded solely by the Funding Transaction. Funds from the Funding Transaction do not become part of a Stored Balance in the Prepaid Account. Funds are transitorily held in the TP Account only until those funds are transferred from the TP Account to the Receiver in the Payment Transaction.
  b. In the Staged Wallet Model, all payments are Intermediated Transfers as there is no Prepaid Account or Stored Balance with the Transfer Provider. Funds from the Funding Transaction are typically held transitorily in a TP Account before being pushed to the Receiver through the Payment Transaction.

III. Relevant Provisions of Regulation E, CFPB FAQs, and Other Guidance

The EFTA and Regulation E set forth error resolution and other obligations for Financial Institutions in relation to electronic fund transfers ("EFTs") that debit or credit a consumer's account.

The CFPB is charged with interpreting and enforcing compliance with the EFTA and Regulation E. The CFPB also issues guidance on Regulation E's requirements, which it typically has done through Supervisory Highlights[6] or the EFT FAQs.[7]

III.A. Regulation E Definitions

III.A.1. Electronic Fund Transfer

An EFT is "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."[8] This includes "transfers resulting from debit card transactions, whether or not initiated through an electronic terminal"[9] and any "transfer sent via ACH."[10] Thus, a Funding Transaction from the Sender's Account at the Sender's Bank to the Transfer Provider, whether through the ACH network or by debit card, is an EFT.

In the EFT FAQs, the CFPB advised that any P2P transfer that meets the definition of an EFT is covered by Regulation E.[11] A P2P transfer that uses a consumer's debit card to transfer funds is an EFT because "the term EFT includes debit card transactions."[12] A credit-push P2P transfer is also an EFT.[13] While the CFPB did not specifically address P2P transfers via ACH, these P2P transfers would also be EFTs because ACH transfers are within the definition of an EFT.

Further, the Intermediated Transfer is an EFT as to the Transfer Provider. When it accepts the Sender's instruction for an Intermediated Transfer, the Transfer Provider agrees to transfer funds from the Sender to the Receiver. As a result, the entire Intermediated Transfer is an EFT as between the Sender and the Transfer Provider because the Intermediated Transfer is a transfer of funds initiated for the purpose of instructing a financial institution (i.e., the Transfer Provider) to debit a consumer's account (i.e., the Sender's Account at the Sender's Bank) in order to fund the transfer to the Receiver.[14] Therefore, where the Transfer Provider agrees with the Sender to transfer funds from the Sender's Account at the Sender's Bank to the Receiver, that entire transfer is an EFT even though the Transfer Provider effects payment to the Receiver via two distinct transactions.

III.A.2. Account

For a transfer to be an EFT, it must debit or credit an "Account", which is (a) "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"[15] and

[6] The Supervisory Highlights are usually published twice per year and are available on the CFPB's website at: https://www.consumerfinance.gov/compliance/supervisory-highlights/.

[7] The EFT FAQs are available on the CFPB's website at: https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/.

[8] 12 C.F.R. § 1005.3(b)(1).

[9] 12 C.F.R. § 1005.3(b)(1)(v).

[10] 12 C.F.R. Part 1005, Supp. I, comment 3(b)(1)-1.ii.

[11] EFT FAQs, Coverage: Transactions, Question 2.

[12] EFT FAQs, Coverage: Transactions, Question 3.

[13] EFT FAQs, Coverage: Transactions, Question 4.

[14] An EFT also includes a "payment made by a bill payer under a bill-payment service available to a consumer via computer or other electronic means, unless the terms of the bill-payment service explicitly state that all payments, or all payments to a particular payee or payees, will be solely by check, draft, or similar paper instrument drawn on the consumer's account." 12 C.F.R. Part 1005, Supp. I, comment 3(b)(1)-1.vi. Similar to Intermediated Transfers, a bill payment provider typically debits the consumer's account for the bill payment and places those funds in an account held by the bill payment provider before sending a credit from the bill payment provider's account to the payee's account. This comment clarifies the transfer of funds from the consumer's account to the third-party payee is an EFT.

[15] 12 C.F.R. § 1005.2(b)(1).

includes (b) a Prepaid Account.[16]

A Prepaid Account includes an account (i) "that is issued on a prepaid basis in a specified amount or not issued on a prepaid basis but capable of being loaded with funds thereafter", (ii) "whose primary function is to conduct transactions with multiple, unaffiliated merchants for goods or services, or at automated teller machines, or to conduct person-to-person transfers," and (iii) "that is not a checking account, share draft account, or negotiable order of withdrawal account."[17] P2P transfers are those where a consumer can send funds via an EFT to another consumer or a business and an account whose primary function is to conduct P2P transfers is a Prepaid Account even if "it is neither redeemable upon presentation at multiple, unaffiliated merchants for goods or services, nor usable at automated teller machines."[18] As a Prepaid Account must be capable of storing funds, a "product, such as a digital wallet, [that] is only capable of storing a consumer's payment credentials for other accounts but is incapable of having funds stored on it, … is not a prepaid account."[19]

The Sender's Account at the Sender's Bank is a deposit account, typically a checking account, and is therefore covered under Regulation E. Under the Prepaid Account model, the Sender also holds an Account with the Transfer Provider that is a Prepaid Account because it is capable of being loaded with funds (e.g., the Stored Balance funded from Sender's Bank or funds received from other Senders), the primary purpose of the account is to conduct P2P transfers or pay merchants, and it is not a checking account. As such, a Prepaid Account issued under the Prepaid Account model also is covered by Regulation E.

III.A.3. Access Device

The definition of an Access Device is important because when a person issues an Access Device and provides EFT services, that person may be considered a Financial Institution. An "Access Device" is "a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers."[20] This includes "debit cards, personal identification numbers (PINs), telephone transfer and telephone bill payment codes, and other means that may be used by a consumer to initiate an [EFT] to or from a consumer account."[21]

In its Supervisory Highlights, the Federal Deposit Insurance Corporation ("FDIC") specifically noted that "a consumer's mobile phone and [money payment platform] EFT application fall under Regulation E's definition of 'access device.'"[22] While the CFPB has not explicitly asserted this position, its guidance suggests support for the FDIC's position. For example, the CFPB concludes in the EFT FAQs that a Transfer Provider is a "financial institution" when it "issues an access device and agrees with a consumer to provide EFT services," and the CFPB goes on to provide the example of a mobile wallet as the type of service that a Transfer Provider could provide that would make it a "financial institution."[23]

Moreover, a username and password approved for use by a Transfer Provider to initiate an EFT through a Transfer Provider's mobile application or website constitute an Access Device as they are a means that the Sender can use to initiate EFTs from the Sender's Account at the Sender's Bank. The Transfer Provider has issued an Access Device once the Sender has established a profile and connected payment credentials (such as a debit card or account and routing number for ACH transfers) to it as that is the point when the mobile application may be used by the Sender to initiate EFTs from the Sender's Account at the Sender's Bank. Depending on the transfer involved, the Access Device can be used to access either the Sender's Account held by the Sender's Bank (e.g., the Sender connects their bank-issued debit card to their Transfer Provider profile for use in Funding Transactions) or the Sender's Prepaid Account held by the Transfer Provider. In either case, the Transfer Provider has issued an Access Device that can be used by the Sender to initiate EFTs.

III.A.4. Financial Institution

Identifying which persons are a Financial Institution in relation to a transaction is important because Financial Institutions are subject to Regulation E's requirements, including those

[16] 12 C.F.R. § 1005.2(b)(3).

[17] 12 C.F.R. § 1005.2(b)(3)(i)(D) (As a Prepaid Account must be capable of storing funds, a "product, such as a digital wallet, [that] is only capable of storing a consumer's payment credentials for other accounts but is incapable of having funds stored on it, … is not a prepaid account.").

[18] 12 C.F.R. Part 1005, Supp. I, comment 2(b)(3)(i)-10.

[19] 12 C.F.R. Part 1005, Supp. I, comment 2(b)(3)(i)-6.

[20] 12 C.F.R. § 1005.2(a)(1).

[21] 12 C.F.R. Part 1005, Supp. I, comment 2(a)-1.

[22] FDIC March 2022 Consumer Compliance Supervisory Highlights, available at: https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/.

[23] EFT FAQs, Coverage: Financial Institutions, Question 2.

relating to error resolution. A "Financial Institution" is (a) a person that "directly or indirectly holds an account belonging to a consumer," ("Part (a)") or (b) a person that "issues an access device and agrees with a consumer to provide electronic fund transfer services" ("Part (b)").[24] While the EFTA and Regulation E do not specifically define what constitutes an "electronic fund transfer service," guidance suggests it is a transfer of funds to or from a person other than the person who issued the access device and is not intended to include transactions initiated by a party solely to collect a payment for goods or services that person provides to the consumer (e.g., a merchant debiting a consumer's account for goods or services the merchant provides to the consumer).[25] As a result, in applying Part (b) of the definition, it is important to determine who is providing the EFT service (e.g., agreeing to transfer funds to or from another person) and the scope of those services.

A Sender's Bank is a Financial Institution under Part (a) of the definition because it holds the Sender's Account, which is the Sender's deposit account. When a Sender's Bank issues a debit card that is used in a Funding Transaction, the Sender's Bank also is a Financial Institution under Part (b) because it has issued an Access Device and agreed with the Sender to provide EFT services. The EFT service the Sender's Bank agrees to provide in this case is to accept and process transactions from merchants who debit the Sender's Account using the debit card information. Therefore, when the Sender's Bank processes an incoming debit to the Sender's Account that transfers funds to the Transfer Provider in the Funding Transaction, it has completed the EFT service it has agreed with the Sender to provide.

A Transfer Provider that meets either part of the definition is also a Financial Institution.[26] A Transfer Provider is a Financial Institution under Part (b) of the definition because it has issued an Access Device and agreed with the Sender to provide EFT services. By way of example of a Financial Institution under Part (b), the CFPB notes in the EFT FAQs that a Transfer Provider "may enter into an agreement with a consumer for a mobile wallet that the consumer can use to initiate debit card transactions from their external bank account to another person's external bank account."[27] As a result, the EFT service the Transfer Provider agrees with the Sender to provide is the Intermediated Transfer. After the Transfer Provider receives funds from the Sender's Bank in the Funding Transaction, it must still execute the Payment Transaction as instructed in order to complete the EFT service it has agreed it to provide (i.e., transfer funds from the Sender to the Receiver).

As discussed further in Section III.D below, from the Sender's perspective, there generally are two Financial Institutions involved in the Funding Transaction and only one Financial Institution involved in the Payment Transaction. Depending on the transfer involved, a P2P Provider may be a Financial Institution under both Part (a) and Part (b) for different parts of a P2P transfer. For example, in a Split-Funded P2P Transfer, the P2P Provider is a Financial Institution under Part (b) of the definition for the Intermediated Transfer portion for the same reasons discussed in the previous paragraph because the P2P Provider is a Transfer Provider as to that portion of the Split-Funded P2P Transfer. The P2P Provider is a Financial Institution under Part (a) of the definition for the Stored Balance Transfer portion of a Split-Funded P2P Transfer because it holds the Sender's Prepaid Account that is debited as part of the Stored Balance Transfer.[28] A P2P Provider can also be a Financial Institution for different reasons depending on the operating model involved. A P2P Provider operating under a Prepaid Account model may be a Financial Institution under Part (a) and Part (b), depending on whether the P2P transfer is an Intermediated Transfer or a Split-Funded P2P Transfer. A Transfer Provider operating under a Staged Wallet model is a Financial Institution only under Part (b). It is important to identify which part of the definition applies as Financial Institutions acting in their capacity under Part (a) cannot be Service Providers.

[24] 12 C.F.R. § 1005.2(i).

[25] 12 C.F.R. Part 1005, Supp. I, comment 7(a)-1 (Explaining that "an agreement with a third party to initiate preauthorized transfers to or from the consumer's account" is a type of EFT service that may trigger disclosures for the Financial Institution holding the consumer's Account); 44 Fed. Reg. 59474 (In discussing the EFT services that may be offered by a Service Provider, the Board of Governors of the Federal Reserve System ("Board") explained "[t]he EFT card issued by [the Service Provider] can be used at automated teller machines (ATMs) and point-of-sale (POS) terminals throughout [the Service Provider's] EFT system by the consumer to receive cash (or make other electronic transfers) and make purchases at merchant locations."). If an EFT service were defined to include transfers to the person issuing the Access Device, nearly every merchant facilitating e-commerce transactions would be considered a Financial Institution because of the broad definition of Access Device (i.e., a profile username and password that can be used through a mobile application or website to direct a transfer of funds from stored debit card or ACH information) and those merchants would have full error resolution obligations for each mobile or web-initiated payment received.

[26] EFT FAQs, Coverage: Financial Institutions, Question 1.

[27] EFT FAQs, Coverage: Financial Institutions, Question 2.

[28] EFT FAQs, Coverage: Financial Institutions, Question 2.

III.A.5. Service Provider

A Financial Institution can also be a Service Provider, in which case it assumes full error resolution obligations for an EFT, while any other Financial Institution involved in the EFT is exempt from investigating and resolving an alleged error. A "Service Provider" is a person that (i) "does not hold the consumer's account," (ii) "issues a debit card (or other access device) that the consumer can use to access the consumer's account held by a financial institution," and (iii) "has no agreement with the account-holding institution regarding such access."[29] A Financial Institution acting in its capacity under Part (a) with respect to a given EFT cannot be a Service Provider because it, by definition, holds the consumer's account that is accessed. A Financial Institution acting in its capacity under Part (b) with respect to a given EFT may be a Service Provider because it issues an Access Device and agrees with the consumer to provide EFT services.[30]

The "account" referenced in the Service Provider definition is the account being accessed by the Access Device (i.e., the Sender's Account at the Sender's Bank in a Funding Transaction) and is not any Account the Service Provider may hold for the same consumer. A Financial Institution may be a Service Provider whether or not it also has established an Account so long as the "account" accessed by the Service Provider's Access Device is an Account held at another Financial Institution.[31]

For example, consider the scenario where a Transfer Provider has established a Prepaid Account for the Sender and the Sender uses the Transfer Provider's Access Device to instruct the Transfer Provider to execute an Intermediated Transfer that is fully funded via a Funding Transaction from the Sender's Account at the Sender's Bank (which is the account-holding financial institution for purposes of clause (i) of the Service Provider definition). The Transfer Provider can be a Service Provider with respect to the Funding Transaction because the Access Device issued by the Transfer Provider accesses the Sender's Account at the Sender's Bank. It does not matter in this scenario that the Transfer Provider holds a Prepaid Account for the Sender because that is not the account being debited in the Funding Transaction.

For a Financial Institution to be a Service Provider with respect to an EFT, it must not have an "agreement" with the account-holding Financial Institution governing the EFT to the account initiated by the Access Device issued by the Service Provider. The ACH rules (i.e., Nacha Rules) alone are not an agreement for purposes of the Service Provider definition.[32] However, the card networks' rules do constitute such an agreement.[33] This distinction arises because of the difference in how the systems operate with regard to Access Devices and the regulatory intent to cover only those agreements that relate to Access Devices. Under the card network rules, a Financial Institution or Transfer Provider (acting as a merchant participant in the card network) is required to honor all debit cards issued on the network as a condition of participating in the network. Card network participants specifically agree to honor each other's Access Devices as part of the network rules and therefore the card network rules are an "agreement."[34] On the other hand, the ACH system does not have such a requirement to honor Access Devices as part of accepting transfers through the system. Thus, participation in and agreement to be bound by rules governing transfers through the ACH system does not constitute an "agreement."[35]

In the scenario described earlier in this section, if the Funding Transaction occurred via ACH, the Transfer Provider would be a Service Provider because it does not hold the account being accessed by the Access Device, has issued an Access Device used for the Funding Transaction, and does not have an agreement with the Sender's Bank regarding the Funding

[29] 12 C.F.R. § 1005.14(a).

[30] 12 C.F.R. § 1005.2(i); EFT FAQs, Coverage: Financial Institutions, Question 1.

[31] 12 C.F.R. Part 1005, Supp. I, comment 14(a)-1.

[32] 12 C.F.R. Part 1005, Supp. I, comment 14(a)-2; EFT FAQs, Coverage: Financial Institutions, Question 1.

[33] EFT FAQs, Coverage: Financial Institutions, Question 4.

[34] 45 Fed. Reg. 8258 ("The Board intends an agreement for these purposes to mean a specific agreement in which two or more institutions agree to provide customers of some or all of them with an EFT service involving an access device, and agree as to their rights and obligations with respect to this service.").

[35] 45 Fed. Reg. 8267 ("Institutions do not have such an agreement solely because they participate in transactions that are cleared through an automated or other clearing house or similar arrangement for the clearing and settlement of fund transfers generally, or because they agree to be bound by the rules of such an arrangement.").

Transaction. In contrast, if the Funding Transaction instead occurred via a debit card transaction, the Transfer Provider cannot be a Service Provider because the card network rules constitute an agreement with the Sender's Bank regarding the debit card transaction.

III.A.6. Unauthorized Electronic Fund Transfer

An "unauthorized electronic fund transfer" is any EFT "from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit."[36] An unauthorized EFT includes an EFT "initiated by a person who obtained the access device from the consumer through fraud or robbery."[37]

In the EFT FAQs, the CFPB explained that an unauthorized EFT includes situations where a "consumer's account access information is obtained from a third party through fraudulent means" and used by the fraudster to conduct an EFT.[38] The CFPB provided the examples of a computer hacker obtaining the consumer's account access information and initiating an EFT from the consumer's account; a consumer sharing debit card information with a P2P payment provider and a fraudster gaining access to the consumer's phone and using the mobile wallet to initiate a transfer from the consumer's deposit or prepaid account; and a thief stealing the consumer's physical wallet and using the debit card to initiate a payment.

The CFPB also explained that "when a consumer is fraudulently induced into sharing account access information with a third party, and a third party uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E."[39] The CFPB provided the examples of a third party posing as a representative from the consumer's financial institution to obtain the consumer's account login information and using that information to initiate an EFT, and a third party using phishing to gain access to a consumer's computer to observe the consumer entering account login information and using that information to initiate an EFT. The CFPB further advised that the EFTs in these examples are not "initiated by a person who was furnished the access device to the consumer's account by the consumer" and instead are "EFTs initiated using account access information obtained through fraud or robbery."[40] Note, however, that these examples contrast with the scenario where the consumer is fraudulently induced into initiating an EFT, which are not unauthorized EFTs because they are not initiated by a person "other than the consumer."

III.A.7. Error

Financial Institutions must investigate and resolve errors asserted by a consumer. An "error" is any of the following:

- "An unauthorized electronic fund transfer;
- An incorrect electronic fund transfer to or from the consumer's account;
- The omission of an electronic fund transfer from a periodic statement;
- A computational or bookkeeping error made by the financial institution relating to an electronic fund transfer;
- The consumer's receipt of an incorrect amount of money from an electronic terminal;
- An electronic fund transfer not identified in accordance with § 1005.9 or § 1005.10(a); or
- 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 an error exists under [§ 1005.11(a)(1)(i) through (vi)]."[41]

The definition of "error" in Regulation E is largely the same as the definition in the EFTA. Other than unauthorized EFTs, which are discussed in Section III.A.6 above, there is little discussion in the regulation or its commentary on the types of issues that fall within each error category. An "incorrect electronic fund transfer" is not defined or further clarified in the EFTA or Regulation E.

[36] 12 C.F.R. § 1005.2(m). An unauthorized EFT does not include an EFT initiated "by a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized." 12 C.F.R. § 1005.2(m). "If a consumer furnishes an access device and grants authority to make transfers to a person (such as a family member or co-worker) who exceeds the authority given, the consumer is fully liable for the transfers unless the consumer has notified the financial institution that transfers by that person are no longer authorized." 12 C.F.R. Part 1005, Supp. I, comment 2(m)-2. An unauthorized EFT also does not include an EFT initiated "with fraudulent intent by the consumer or any person acting in concert with the consumer" or "by the financial institution or its employee." 12 C.F.R. § 1005.2(m).

[37] 12 C.F.R. Part 1005, Supp. I, comment 2(m)-3.

[38] EFT FAQs, Error Resolution: Unauthorized EFTs, Question 4.

[39] EFT FAQs, Error Resolution: Unauthorized EFTs, Question 5.

[40] EFT FAQs, Error Resolution: Unauthorized EFTs, Question 6.

[41] 12 C.F.R. § 1005.11(a)(1). An "error" does not include any of the following: "a routine inquiry about the consumer's account balance; a request for information for tax or other record keeping purposes; or a request for duplicate copies of documentation." 12 C.F.R. § 1005.11(a)(2).

III.B. Requirements for Error Resolution for Financial Institutions

III.B.1. Overview of Error Resolution Procedures[42]

Upon timely receipt of a notice of error from a consumer, a Financial Institution must promptly investigate and resolve the error.[43] Regulation E imposes requirements for how long a Financial Institution has to complete its investigation, the steps a Financial Institution must take when its investigation reveals an error occurred, and the procedures a Financial Institution must follow when its investigation reveals no error or a different error occurred. If the error involves an unauthorized EFT, Regulation E provides that the consumer may be held liable for some portion of the EFT based on when the consumer provided notice to the Financial Institution of the unauthorized EFT.[44]

III.B.2. Consumer Notice Triggering Error Resolution Obligations

A Financial Institution's error resolution obligations are triggered when the consumer provides notice of an error.[45] The consumer has 60 days from the date the Financial Institution sent the periodic statement on which the error was first reflected to provide notice of the alleged error to the Financial Institution.[46] The notice must include information sufficient for the Financial Institution to identify the consumer and account number and must indicate why the consumer believes an error exists.[47]

General assertions by the consumer are sufficient to trigger the Financial Institution's error resolution obligations. Regulation E notes that additional information about the error, such as the type, date, and amount, only needs to be provided by the consumer "to the extent possible."[48] A broad interpretation of a consumer's notice helps ensure consumers receive the benefits of the regulation's requirements even if consumers are unable to provide specific details about an alleged error.[49] However, a Financial Institution may struggle with what constitutes an error assertion given the lack of clarity about the types of issues that fall within certain error categories. For example, a Financial Institution may find it difficult to determine whether a consumer notice has asserted an incorrect EFT as Regulation E provides no definition or explanation of the factual situations that constitute incorrect EFTs.[50]

The broad guidance on what constitutes an error assertion may also lead a Financial Institution to be overinclusive in the types of claims it treats as errors because of a lack of information provided in the initial error notice. For example, a consumer who purchases goods online and is dissatisfied with the goods when they arrive may inform the Financial Institution that the purchase is unauthorized but omit the fact that the consumer, in fact, made the purchase. In such cases, the Financial Institution treats the claim as an error and begins its investigation. When the investigation reveals the consumer made the purchase, the investigation concludes with a finding that no error occurred. In contrast, if the same consumer informed the Financial Institution that the consumer purchased the goods but wishes to dispute the purchase because the consumer is unable to obtain a refund from the retailer, the Financial Institution would treat the consumer as having not asserted an error and would not be required to investigate the issue under Regulation E.

A Financial Institution can ask consumers for more information about an alleged error, but it cannot delay the investigation until it receives such information.[51] For example, a Financial Institution may request an affidavit or police

[42] More detailed information about the error resolution procedures is set forth in Appendix A.

[43] 12 C.F.R. § 1005.11(b), (c), and (d).

[44] 12 C.F.R. § 1005.6(b).

[45] 12 C.F.R. § 1005.11(b)(1). When a consumer asks whether an EFT was debited or credited to the Account without actually asserting any error, the error resolution procedures do not apply. 12 C.F.R. Part 1005, Supp. I, comment 11(a)-2. A consumer's notice of loss or theft of an access devices also does not trigger the error resolution procedures unless the consumer also "alleges possible unauthorized use as a consequence of the loss or theft." 12 C.F.R. Part 1005, Supp. I, comment 11(a)-3.

[46] 12 C.F.R. § 1005.11(b)(1)(i).

[47] 12 C.F.R. § 1005.11(b)(1)(ii) and (iii).

[48] 12 C.F.R. § 1005.11(b)(1)(iii).

[49] 44 Fed. Reg. 59481 ("The commentary to the first proposal suggested that a financial institution would not be relieved of error resolution responsibilities where a consumer is unable to describe the error or articulate the amount of or the reasons for the error. . . The Board still believes that its position is proper and necessary in order to minimize the possibility that a consumer could be denied the protections of section 205.11 by not being able to understand the cause or nature of the error or articulate the reasons for the error. Consequently, where a consumer's notification is somewhat vague or imprecise, a financial institution is expected to make a good faith effort to identify and resolve the alleged error.").

[50] In such cases, a Financial Institution may elect to initially treat a consumer's claim as a non-Regulation E complaint in order to investigate and determine whether there is any issue with the account.

[51] 12 C.F.R. Part 1005, Supp. I, comment 11(b)(1)-2.

report from the consumer but the Financial Institution "may not delay initiating or completing an investigation pending receipt of [such] information…"[52]

III.C. Requirements for Error Resolution for Transfers Involving Service Providers

III.C.1. The Service Provider Has Full Error Resolution Obligations

When a consumer provides notice of an error to a Service Provider regarding an EFT initiated via the Access Device issued by the Service Provider, the Service Provider must comply with the full error resolution obligations as set forth in Section III.B and Appendix A. As the party issuing the Access Device, the Servicer Provider should bear the risks associated with such issuance and, therefore, the Service Provider is assigned responsibility for error resolution and the account-holding Financial Institution's error resolution obligations are very limited as described in Section III.C.2 below.

While the full error resolution obligations apply, there are some differences in relation to Service Providers. The Service Provider must extend the time a consumer has to submit a notice of error by a reasonable time if the consumer is delayed in providing notice because they first attempted to notify the account-holding Financial Institution.[53] If a Service Provider must provide provisional credit, it must, in addition to the other required disclosures, tell the consumer the date on which it initiated the transfer for provisional credit.[54] If a Service Provider will debit a provisional credit because the investigation revealed no error occurred, it must notify the account-holding Financial Institution of the period during which the account-holding Financial Institution must honor debits to the account.[55] The Service Provider is responsible to the account-holding Financial Institution for the amount of any overdraft that results from the debiting of the provisional credit.[56]

When an investigation reveals an error occurred, the amount of the error correction provided by the Service Provider must include all fees and charges imposed by either the Service Provider or the account-holding Financial Institution.[57] The Service Provider must also comply with the general error resolution procedures outlined in section 1005.11, which requires the amount of the error correction to include interest, if applicable.[58] As Regulation E assigns full responsibility for error correction to the Service Provider, the Transfer Provider is likely liable to the Sender for any interest due if the Sender's Account at the Sender's Bank is an interest-bearing account. As discussed further in Section III.C.2 below, the account-holding Financial Institution is required to provide, upon request, information needed by the Service Provider in connection with an error investigation. If the Sender's Bank receives such a request, from either the Sender or the Transfer Provider, the Sender's Bank must provide information about interest and fees that should be included in the amount of the error correction. Even if the Sender's Bank does not receive such a request, it may still provide information about interest and fees to the Sender so that the Sender can provide such information to the Transfer Provider in connection with the error claim.

One issue that arises in the context of Transfer Providers operating under the Prepaid Account model that are Service Providers is whether the Transfer Provider can credit the Sender's Prepaid Account rather than the Sender's Account at the Sender's Bank. When providing provisional credit or correcting an error, the Transfer Provider must credit "the consumer's account."[59] The consumer account involved in the Intermediated Transfer is the Sender's Account at the Sender's Bank. Therefore, Regulation E implies that the account that must be credited is the Sender's Account at the Sender's Bank. Further, a Transfer Provider is required to notify the Sender's Bank when it debits a provisional credit, which further supports that the Sender's Account at the Sender's Bank is the account that must be credited. However, because Regulation E does not expressly require the Service Provider investigating the error to credit the Account that was debited in connection with the alleged erroneous EFT, there may be cases where a Transfer Provider credits the Sender's Prepaid Account instead.

III.C.2. Account-holding Financial Institution Has Limited Error Resolution Obligations

While the account-holding Financial Institution does not

[52] EFT FAQs, Error Resolution, Question 4.

[53] 12 C.F.R. § 1005.14(b)(2)(i).

[54] 12 C.F.R. § 1005.14(b)(2)(ii).

[55] 12 C.F.R. § 1005.14(b)(2)(iv).

[56] 12 C.F.R. § 1005.14(b)(2)(iv).

[57] 12 C.F.R. Part 1005, Supp. I, comment 14(b)(2)-1.

[58] 12 C.F.R. Part 1005, Supp. I, comment 11(c)-6.

[59] 12 C.F.R. § 1005.11(c)(2)(i), 1005.14(b)(2)(iii).

have full error resolution obligations, it does have to follow two rules. First, upon request, the account-holding Financial Institution must provide information or copies of documents that the Service Provider needs to investigate errors or to furnish copies of documents to the consumer.[60] Second, when the Service Provider will debit a provisional credit, the account-holding Financial Institution must also honor all checks, drafts, or similar instruments payable to third parties and preauthorized EFTs from the Account for five business days after the Service Provider notifies the consumer of that the provisional credit will be debited.[61]

III.D. Error Resolution Responsibilities of the Transfer Provider and the Sender's Bank

This section addresses how the error resolution requirements discussed above in Section III.B and III.C, and in Appendix A, apply to the Sender's Bank and the Transfer Provider for Funding Transactions, Payment Transactions, and Intermediated Transfers. Sections III.D.1, III.D.2 and III.D.3 explain when the Sender's Bank, Transfer Provider, or both are Financial Institutions as a general matter and, thus, have error resolution obligations. Sections III.D.1.a and III.D.1.b describe potential factual variations that impact the parties' error resolution obligations.

III.D.1. The Transfer Provider and the Sender's Bank Both Are Financial Institutions with Respect to Funding Transactions

For purposes of the Funding Transaction of an Intermediated Transfer, both the Sender's Bank and the Transfer Provider are Financial Institutions. The Sender's Bank holds the Sender's Account being debited and is therefore a Financial Institution under Part (a). The Transfer Provider is a Financial Institution under Part (b) because it issues an Access Device to the Sender and agrees to provide EFT services, and, further, it does not hold the Account being debited. Since the Transfer Provider is covered under Part (b), it may also be a Service Provider if it does not have an agreement with the Sender's Bank regarding the type of EFT used for the Funding Transaction.

That there are two Financial Institutions involved does not alleviate either of its Regulation E error resolution obligations. If a consumer provides timely notice of an error to either Financial Institution, that Financial Institution must comply with its error resolution obligations.[62] If the Sender provides timely notice of an error to both the Sender's Bank and the Transfer Provider, both have full error resolution obligations, as discussed in Section III.B above and Appendix A. Each must investigate promptly and cannot require the Sender to first try to resolve the error with the other Financial Institution.[63] The only exception is when the Transfer Provider is a Service Provider, as discussed in Section III.D.1.b below.

III.D.1.a. The Transfer Provider Resolves the Error Pertaining to the Funding Transaction when the Transfer Provider is not a Service Provider

When both the Sender's Bank and the Transfer Provider have error resolution obligations for a Funding Transaction because the Transfer Provider is not a Service Provider, it is possible that the Transfer Provider will correct the error before the Sender's Bank has finalized its investigation. When that occurs, the Sender's Bank may use that information as part of its investigation and resolution of the Sender's claim. The Sender's Bank must still report the results of the investigation to the Sender, but it would not need to also correct the error. While the CFPB has not directly stated this outcome for errors involving EFTs, it has done so in other rules, including in other parts of Regulation E, so it is reasonable to conclude that the CFPB would not object if the Sender's Bank does not also credit the Sender's Account for an error after the Transfer Provider has corrected the same error.[64]

For example, consider a scenario where the Sender asserts the same error with a Funding Transaction to both the

[60] 12 C.F.R. § 1005.14(c)(2).

[61] 12 C.F.R. § 1005.14(c)(2). Only those items that would have been paid if the provisional credit had not been debited need to be honored. 12 C.F.R. § 1005.11(d)(2)(ii).

[62] EFT FAQs, Coverage: Financial Institutions, Question 1 ("Any entity that is considered a financial institution under Regulation E has error resolution obligations in the event that a consumer notifies the financial institution of an error"); EFT FAQs, Error Resolution: Unauthorized EFTs, Question 4 ("All of the financial institutions in these examples, including any non-bank P2P payment provider or deposit account holding financial institution, must comply with the error resolution requirements").

[63] EFT FAQs, Error Resolution: Unauthorized EFTs, Question 9.

[64] In the remittance transfer error resolution rules, the CFPB explained that if a remittance transfer provider or an account-holding institution provides a credit for an error asserted to both parties, the other party "has no further responsibilities to investigate the error if the error has been corrected." 12 C.F.R. Part 1005, Supp. I, comment 33(f)-3. In the credit card error resolution rules under Regulation Z, the CFPB explained a creditor may reverse amounts previously credited to correct an error if the consumer "receives more than one credit to correct the same billing error" as long as "the total amount of the remaining credits is equal to or more than the amount of the error and that the consumer does not incur any fees or other charges as a result of the timing of the creditor's reversal." 12 C.F.R. Part 1026, Supp. I, comment 13(c)(2).

Sender's Bank and the Transfer Provider, triggering error resolution obligations for both parties. The Sender's Bank and the Transfer Provider each start an error investigation. The Transfer Provider confirms an error with respect to the Funding Transaction and corrects the error by transferring funds to the Sender's Account at the Sender's Bank. The Sender's Bank may point to the fact that the Transfer Provider corrected the error to conclude the error has been resolved. The Sender's Bank should then provide notice to the Sender that the investigation is complete and that the error has been corrected by the Transfer Provider.

The outcome would be the same even if the Sender Bank's had provided a provisional credit to the Sender's Account. The Sender's Bank would still be required to provide notice and comply with the Regulation E requirements regarding debiting a provisional credit, but it could point to the Transfer Provider's credit to show the error was properly corrected.

When a Transfer Provider operates under the Prepaid Account model, Regulation E and related guidance do not expressly address whether the Transfer Provider can credit the Sender's Prepaid Account rather than the Sender's Account at the Sender's Bank to correct an error. The provisional credit requirements under Regulation E provide that the Transfer Provider must credit "the consumer's account."[65] The consumer account involved in the Intermediated Transfer is the Sender's Account at the Sender's Bank. Therefore, Regulation E implies that the account that must be provisionally credited is the Sender's Account at the Sender's Bank. However, the requirements of Regulation E governing final correction of an error provide only that the Transfer Provider must "correct the error within one business day after determining that an error occurred,"[66] and generally do not mandate the action the Transfer Provider must take to correct the error. Unlike the provisional credit rules, the error correction rules do not reference crediting a consumer's account. If corrective action involves a refund to the Sender (e.g., the error involves an unauthorized EFT or an EFT in excess of the amount the Sender authorized), a Transfer Provider may believe it satisfies Regulation E by crediting the Sender's Prepaid Account for provisional and final credits and need not provide the credit to the Sender's Account at the Sender's Bank.

Additionally, when an investigation reveals an error occurred, the correction must include interest and fees, if applicable.[67] Regulation E does not specify whether this includes interest and fees assessed or paid by the Sender's Bank, interest and fees assessed or paid by the Transfer Provider or both. Regulation E explains that "[i]f a financial institution determines an error occurred, … it must correct the error … including, where applicable, the crediting of interest and the refunding of any fees imposed by the institution."[68] Other than in the rules for Service Providers discussed in Section III.C.1, Regulation E's general error resolution rules do not contemplate scenarios where there are two Financial Institutions responsible for error resolution as to the same EFT and therefore do not address any requirements for one Financial Institution to reimburse interest or fees assessed or paid by the other Financial Institution involved. Where neither Financial Institution is a Service Provider, Regulation E also does not impose any requirement for the two Financial Institutions to share information about the underlying EFT subject to an error claim and any related interest and fees. As a result, a Transfer Provider may be unaware of interest or fees assessed or paid by the Sender's Bank and may not include such amounts when correcting an error, even if the error is corrected as a refund to the Sender's account at the Sender's Bank.

The risks of relying on the Transfer Provider's error correction likely increase where the Sender's Bank is unsure whether the Transfer Provider credited the Sender for the error (e.g., if the Transfer Provided credited the Sender's Prepaid Account). If the Sender's Bank is able to confirm that the Transfer Provider credited the Sender's Prepaid Account for an error and the amount of the credit, the Sender's Bank likely may rely on that information to resolve the Sender's claim without also having to credit the Sender's Account. However, if the Sender's Bank knows the error was corrected but is unable to confirm the details of the credit, it may need to make a risk-based decision on whether it has sufficient information to show the error was corrected.

A Transfer Provider may also determine that the amount of the error was different than that asserted by the Sender or be unaware of any interest or fees imposed by the Sender's Bank in connection with the alleged erroneous transaction, resulting in a credit by the Transfer Provider for less than the full amount due in connection with the error. In such cases, the Sender's Bank likely is responsible to the Sender

[65] 12 C.F.R. § 1005.11(c)(2)(i).

[66] 12 C.F.R. § 1005.11(c)(1), (c)(2)(iii).

[67] 12 C.F.R. Part 1005, Supp. I, comment 11(c)-6.

[68] *Id.*

for the deficiency but can still point to the Transfer Provider's correction for the other amounts.

III.D.1.b. The Transfer Provider is a Service Provider

When the Transfer Provider is a Service Provider, the Sender's Bank has more limited error resolution obligations. As discussed in Section III.A.5 above, the Transfer Provider, which has issued an Access Device to the Sender, is a Service Provider when there is no agreement between it and the Sender's Bank regarding the Funding Transaction. In that case, as the account-holding Financial Institution, the Sender's Bank is only required to provide information and copies of documentation and to honor items and preauthorized EFTs in connection with the debiting of a provisional credit, as discussed in Section III.C.2 above. While not explicitly required, the Sender's Bank may advise the Sender to provide notice of the alleged error to the Transfer Provider. Further, the Sender's Bank is not itself required to notify the Transfer Provider of an alleged error.

The Transfer Provider, as the Service Provider, has full error resolution obligations, as discussed in Section III.C.1 above. The Transfer Provider is responsible for investigating the Sender's claim, determining whether an error occurred, correcting any error, and notifying the Sender of the results of the investigation. The Sender's Account at the Sender's Bank should be credited for any error but, in some cases, a Transfer Provider might credit the Sender's Prepaid Account for the amount of the error rather than crediting the Sender's Account at the Sender's Bank (even though this may be inconsistent with Regulation E). The Transfer Provider is also responsible for any interest and fees assessed by the Sender's Bank in connection with the alleged erroneous EFT.

III.D.2. Only the Transfer Provider is a Financial Institution with Respect to the Payment Transaction

As the Payment Transaction of an Intermediated Transfer involves the transfer of funds between the TP Account and the Receiver's account, the Transfer Provider is a Financial Institution as to the Sender regarding the Payment Transaction because it is part of the Intermediated Transfer EFT service the Transfer Provider has agreed with the Sender to provide. The Sender's Bank is not a Financial Institution for the Payment Transaction as the Sender's Bank does not hold a consumer account being debited or credited as part of the Payment Transaction and has not agreed with a consumer to provide EFT services related to the Payment Transaction, so it does not have any error resolution obligations. The Receiver's bank may also be a Financial Institution for a Payment Transaction but would not have error resolution obligations under Regulation E as to any error claim by the Sender.[69] The Transfer Provider is the Financial Institution with responsibility for the Payment Transaction for any notice of error provided by the Sender that implicates that transaction. The Sender's Bank is not responsible for the Payment Transaction nor does it have any error resolution obligation with respect to any disputes involving the Payment Transaction.

III.D.3. Only the Transfer Provider is a Financial Institution with Respect to the Intermediated Transfer

When a Transfer Provider executes a Sender's instruction via an Intermediated Transfer, it agrees with the Sender to transfer funds from the Sender's Account at the Sender's Bank to the Receiver. As a result, the entire Intermediated Transfer is an EFT as between the Sender and the Transfer Provider because the Intermediated Transfer is a "transfer of funds initiated … for the purpose of … instructing … a financial institution [(i.e., the Transfer Provider)] to debit … a consumer's account [(i.e., the Sender's Account at the Sender's Bank)]" in order to fund the transfer to the Receiver. The Sender's instruction to the Transfer Provider is not complete until funds have been transferred from the Sender's Account at the Sender's Bank to the Receiver. If the Transfer Provider fails to execute the Sender's full instruction due to an occurrence constituting an "error" under Regulation E, the Transfer Provider has error resolution obligations as to the Intermediated Transfer regardless of whether the occurrence constituting the "error" is isolated to the Funding Transaction or the Payment Transaction.[70]

In contrast, the Sender's instruction to the Transfer Provider that is passed on to the Sender's Bank is limited to transferring funds from the Sender's Account to the Transfer Provider by properly processing the incoming debit (i.e., the Funding Transaction). The Sender's Bank is not privy to any further instructions between the Sender and the Transfer Provider (including as to the Payment Transaction). As a result, the Sender's Bank is only responsible for the Funding Transaction.

[69] The Receiver's bank could have error resolution obligations for a claim of error submitted by the Receiver (assuming the Receiver is a consumer), if, for example, the EFT was not properly reflected on the Receiver's periodic statement. Also, note that if the Sender's Bank also happens to be the Receiver's bank, it may be a Financial Institution for the Payment Transaction. However, it would be a Financial Institution in its capacity as the Receiver's bank and not in its capacity as the Sender's Bank.

[70] For an example of the applicability of this principle, see Section IV.D.1 and IV.D.2.

IV. Error Scenarios and Error Resolution Obligations in Intermediated Transfers

In each scenario below, the "Consumer" is the person who opened an account with a depository financial institution ("Consumer's Bank"). When a Consumer authorizes an Intermediated Transfer, the Consumer is a Sender and the Consumer's Bank is the Sender's Bank. Each of the scenarios considered below assumes the following basic facts and funds flows:

- Each Intermediated Transfer is initiated through the Transfer Provider (e.g., using the Access Device issued by the Transfer Provider) and not the Consumer's Bank.
- Funds are pulled from the Consumer's Account at the Consumer's Bank via a debit transfer (i.e., for the Funding Transaction).
- The funds for the Intermediated Transfer move from the Consumer's account at the Consumer's Bank to a TP Account at the conclusion of the Funding Transaction (i.e., the funds debited from the Consumer's Bank are not used to fund a Stored Balance in a Prepaid Account at the Transfer Provider but rather are used to fund an Intermediated Transfer).
- A Consumer challenging an Intermediated Transfer provides timely notice of the alleged error to the Consumer's Bank in accordance with Regulation E.
- The Consumer's error notice sets forth all the facts outlined in each scenario and such facts are true.[71]

IV.A. Fraudster Initiates Intermediated Transfers Using Stolen Credentials

IV.A.1. A Fraudster Obtains Transfer Provider Access Device Without the Consumer's Knowledge – Baseline Scenario (Debit Card)

The Consumer has a Prepaid Account or Wallet relationship with a Transfer Provider. The Consumer has provided debit card information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions. A fraudster gains direct access to the Consumer's Transfer Provider Access Device without the Consumer's participation or knowledge, such as by hacking into the Consumer's phone or observing the Consumer input their login credentials. The fraudster instructs the Transfer Provider to transfer funds to the fraudster's bank account and the Transfer Provider executes that instruction via an Intermediated Transfer.

IV.A.1.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction is an unauthorized EFT because the Transfer Provider did not have "actual authority" to initiate EFTs from the Consumer's account at the Consumer's Bank. The fraudster is unable to give such authority to the Transfer Provider because the Fraudster is not an accountholder authorized to transact on the Consumer's account at the Consumer's Bank, is not an authorized user of the access device issued by the Transfer Provider, or otherwise acting on behalf of the Consumer. That the fraudster gained access to the Consumer's account at the Consumer's Bank through the Transfer Provider does not impact whether the fraudster has authority to authorize EFTs from such account. Further, even if the Consumer provided a standing authorization when establishing the relationship with the Transfer Provider, the Consumer is still required to give additional instruction (date, amount, receiver, etc.) to the Transfer Provider before any authorized Intermediated Transfer under the standing authorization can be facilitated. If the Consumer is not the person who gives such instruction to the Transfer Provider, the Intermediated Transfer is unauthorized. The Consumer has asserted an error to the Consumer's Bank.

IV.A.1.b. The Consumer's Bank's Error Resolution Obligations

The Consumer's Bank has full error resolution obligations for the Funding Transaction under this scenario because the Transfer Provider is not a Service Provider. As discussed in Section III.A.5 above, in order to be a Service Provider, the Transfer Provider must not have an agreement in place with the Consumer's Bank. As the Funding Transaction in this scenario involved a debit card transaction, the Transfer

[71] For purposes of this paper, the Consumer is assumed to provide a full, accurate account of the alleged error. However, as a practical matter, this often does not occur in real notices of error and related investigations. As discussed in Section III.B.2, the facts a Consumer alleges may not be as clear as the scenarios in this paper or may not fully come to light until later in the Financial Institution's investigation.

Provider and the Consumer's Bank have an agreement in place (i.e., the card network rules) regarding the Funding Transaction. Therefore, the Consumer's Bank cannot rely on the Service Provider rules under Regulation E.

As the Transfer Provider is also a Financial Institution with respect to the Funding Transaction, the Consumer may also submit an error claim to the Transfer Provider. However, this does not alleviate the Consumer's Bank of its error resolution obligations, and the Consumer's Bank may not condition compliance with its error resolution obligations on the Consumer asserting an error with the Transfer Provider.

IV.A.1.c. The Transfer Provider's Error Resolution Obligations

The Funding Transaction is unauthorized as to the Transfer Provider because it was initiated by a person without authority to initiate transfers from the Consumer's account at the Consumer's Bank. As a Financial Institution with respect to the Funding Transaction, the Transfer Provider has full error resolution obligations.

IV.A.1.d. Interbank Recovery Options

Where a Consumer denies authorizing or participating in the Funding Transaction, the Consumer's Bank may charge back (i.e., return) the debit card transaction under the applicable card network rules. The card network rules permit the Consumer's Bank to initiate a chargeback of a debit card transaction for fraud within 120 calendar days from the transaction date. The Transfer Provider's merchant acquiring bank then must absorb the loss for the amount of the debit card transaction, unless it can show it has issued a refund or the transaction was authorized.[72] Typically, the Transfer Provider's bank passes through these losses and responsibilities to the Transfer Provider by contract.[73] This process happens outside the scope of Regulation E and the Consumer's Bank's ability to charge back the transaction has no impact on its Regulation E obligations.

[72] As discussed further in Section V, even if the Consumer's Bank has the ability to initiate a chargeback for a debit card transaction, the Consumer's Bank is not guaranteed ultimate recovery of the funds. For example, the Transfer Provider may re-present the chargeback if it believes the transaction was authorized. If the Consumer has not submitted an error notice to the Transfer Provider, the Transfer Provider's standard for determining whether the transfer is authorized may be different than the required standard under Regulation E for unauthorized EFTs.

[73] If the Transfer Provider is liable for the debit card transaction, the Receiver will have a windfall (and perhaps ill-gotten) gain unless the Transfer Provider is able to recover the funds from the Receiver. The EFTA and Regulation E do not provide for any such recovery, although the Transfer Provider may be able to leverage its agreement with the Receiver, payment network rules, or other legal action to recover.

IV.A.2. A Fraudster Obtains Transfer Provider Access Device without the Consumer's Knowledge – Scenario Variation 2 (ACH Debit)

The facts are the same as in the Baseline Scenario (IV.A.1) except the Consumer has provided ACH information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions.

IV.A.2.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction will be considered an unauthorized EFT for the same reasons as discussed in the Baseline Scenario. The Consumer has asserted an error to the Consumer's Bank.

IV.A.2.b. The Consumer's Bank's Error Resolution Obligations

The Consumer's Bank will not have full error resolution obligations for the Funding Transaction under this scenario because the Transfer Provider is a Service Provider. The Transfer Provider does not hold the account being debited for the Funding Transaction, has issued an access device that can access the Consumer's account at the Consumer's Bank, and the Transfer Provider and the Consumer's Bank do not have an agreement in place regarding the Funding Transaction because, as discussed in Section III.A.5 above, the Nacha Rules do not constitute an agreement. Therefore, the Consumer's Bank's error resolution responsibilities are limited to those described above in Section III.C.2.

IV.A.2.c. The Transfer Provider's Error Resolution Obligations

The Funding Transaction is unauthorized as to the Transfer Provider for the same reasons as discussed in the Baseline Scenario. As a Financial Institution with respect to the Funding Transaction, the Transfer Provider has full error resolution obligations. As the Transfer Provider is also a Service Provider, the full error resolution obligations as discussed in Section III.C.1 will apply.

IV.A.2.d. Interbank Recovery Options

Even though the Consumer's Bank does not have full error resolution obligations, where a Consumer denies authorizing or participating in the Funding Transaction, the Consumer's Bank may return the ACH debit under the Nacha Rules. The Nacha Rules permit the Consumer's Bank to return

an unauthorized ACH debit within 60 calendar days from the Settlement Date[74] of the transfer if it obtains a Written Statement of Unauthorized Debit from the Consumer and credits the Consumer's account for the amount of the returned ACH debit. The Transfer Provider's bank that originated the unauthorized debit must refund the amount of that transfer to the Consumer's Bank. Typically, the Transfer Provider's bank passes through the financial loss associated with such returns to the Transfer Provider. This process happens outside the scope of Regulation E.

IV.B. Fraudulent Inducement

IV.B.1. Fraudulent Inducement to Share Transfer Provider Access Device – Baseline Scenario (Debit Card)

The Consumer has a Prepaid Account or Wallet relationship with a Transfer Provider. The Consumer has provided debit card information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions. A fraudster tricks the Consumer into sharing the Access Device (e.g., the Consumer's username and password to their Prepaid Account or Wallet) enabled by Transfer Provider for use in initiating EFTs through the Transfer Provider. The fraudster uses the Access Device to instruct the Transfer Provider to transfer funds to the fraudster's bank account and the Transfer Provider executes that instruction via an Intermediated Transfer.

IV.B.1.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction in this scenario is an unauthorized EFT as the Transfer Provider did not have "actual authority" to initiate EFTs from the Consumer's account at the Consumer's Bank. Even though the Consumer provided the access device to the fraudster, the fraudster is unable to give such authority to the Transfer Provider because the fraudster obtained such device via fraud. As discussed above in Section III.A.6, the commentary specifically notes EFTs initiated by a person who "obtained the access device from the consumer through fraud or robbery" are unauthorized EFTs. The CFPB has further advised this remains the case even when a Consumer voluntarily provides the information to a fraudster.[75] The Consumer has asserted an error to the Consumer's Bank.

IV.B.1.b. The Consumer's Bank's Error Resolution Obligations

The Consumer's Bank has full error resolution obligations for the Funding Transaction under this scenario because the Transfer Provider is not a Service Provider. As discussed in Section III.A.5 above, in order to be a Service Provider, the Transfer Provider must not have an agreement in place with the Consumer's Bank. As the Funding Transaction in this scenario involved a debit card transaction, the Transfer Provider and the Consumer's Bank have an agreement in place (i.e., the card network rules) regarding the Funding Transaction. Therefore, the Consumer's Bank cannot rely on the Service Provider rules under Regulation E.[76]

As the Transfer Provider is also a Financial Institution with respect to the Funding Transaction, the Consumer may also submit an error claim to the Transfer Provider. However, this does not alleviate the Consumer's Bank of its error resolution obligations, and the Consumer's Bank may not condition compliance with its error resolution obligations on the Consumer asserting an error with the Transfer Provider.

IV.B.1.c. The Transfer Provider's Error Resolution Obligations

The Funding Transaction is unauthorized as to the Transfer Provider because it was initiated by a person without actual authority to initiate transfers from the Consumer's account at the Consumer's Bank. As a Financial Institution with respect to the Funding Transaction, the Transfer Provider has full error resolution obligations.

IV.B.1.d. Interbank Recovery Options

Where a Consumer denies authorizing or participating in the Funding Transaction, the Consumer's Bank may charge back (i.e., return) the debit card transaction under the applicable card network rules. The card network rules permit the Consumer's Bank to initiate a chargeback of a debit card transaction for fraud within 120 calendar days from the transaction date. The Transfer Provider's merchant acquiring bank then must absorb the loss for the amount of the debit card transaction, unless it can show it has issued a refund or the transaction was authorized. Typically, the Transfer Provider's bank passes through these losses and responsibilities to the Transfer Provider by contract. This process happens outside the scope of Regulation E and the Consumer's Bank's ability to charge back the transaction has no impact on its Regulation E obligations.

[74] Under the Nacha Rules, the Settlement Date is "the date an exchange of funds with respect to an Entry is reflected on the books of the applicable Federal Reserve Bank(s)." Nacha Rules Section 8.103.

[75] EFT FAQs, Error Resolution: Unauthorized EFTs, Question 5.

[76] EFT FAQs, Financial Institutions, Question 4.

IV.B.2. Fraudulent Inducement to Share Transfer Provider Access Device – Scenario Variation 2 (ACH Debit)

The facts are the same as in the Baseline Scenario (IV.B.1) except the Consumer has provided ACH information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions.

IV.B.2.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction in this scenario is an unauthorized EFT for the same reasons as discussed in the Baseline Scenario. The Consumer has asserted an error to the Consumer's Bank.

IV.B.2.b. The Consumer's Bank's Error Resolution Obligations

The Consumer's Bank will not have full error resolution obligations for the Funding Transaction under this scenario because the Transfer Provider is a Service Provider. The Transfer Provider does not hold the account being debited for the Funding Transaction, has issued an access device that can access the Consumer's account at the Consumer's Bank, and the Transfer Provider and the Consumer's Bank do not have an agreement in place regarding the Funding Transaction because, as discussed in Section III.A.5 above, the Nacha Rules do not constitute an agreement. Therefore, the Consumer's Bank's error resolution responsibilities are limited to those described above in Section III.C.2.

IV.B.2.c. The Transfer Provider's Error Resolution Obligations

The Funding Transaction is unauthorized as to the Transfer Provider for the same reasons as discussed in the Baseline Scenario. As a Financial Institution with respect to the Funding Transaction, the Transfer Provider has full error resolution obligations. As the Transfer Provider is also a Service Provider, the full error resolution obligations as discussed in Section III.C.1 will apply.

IV.B.2.d. Interbank Recovery Options

Even though the Consumer's Bank does not have full error resolution obligations, where a Consumer denies authorizing or participating in the Funding Transaction, the Consumer's Bank may return the ACH debit under the Nacha Rules. The Nacha Rules permit the Consumer's Bank to return an unauthorized ACH debit within 60 calendar days from the Settlement Date of the transfer if it obtains a Written Statement of Unauthorized Debit from the Consumer and credits the Consumer's account for the amount of the returned ACH debit. The Transfer Provider's bank that originated the unauthorized debit must refund the amount of that transfer to the Consumer's Bank. Typically, the Transfer Provider's bank passes through the financial loss associated with such returns to the Transfer Provider. This process happens outside the scope of Regulation E.

IV.B.3. Fraudulent Inducement to Transfer Funds Through Intermediated Transfer – Scenario Variation 3 (Debit card)[77]

The Consumer has a Prepaid Account or Wallet relationship with a Transfer Provider. The Consumer has provided debit card information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions. A fraudster tricks the Consumer into initiating an Intermediated Transfer to pay for goods or services the fraudster never intends to provide. The Consumer instructs the Transfer Provider to transfer funds to the fraudster's bank account and the Transfer Provider executes that instruction via an Intermediated Transfer. The Consumer never receives the goods or services.

IV.B.3.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction is not an unauthorized EFT because the Consumer specifically directed the Transfer Provider to pay the fraudster and, in so directing, also authorized the Transfer Provider to make the Funding Transaction through a debit to the Consumer's account at the Consumer's Bank through the debit card on file with the Transfer Provider. As discussed above in Section III.A.6, an unauthorized EFT must be "initiated by a person other than the consumer without actual authority to initiate the transfer." The Consumer's claim also does not fall within any of the other error categories discussed in Section III.A.7. The Consumer has not asserted an error to the Consumer's Bank.

[77] Had the Funding Transaction been made via an ACH debit, the outcome would be the same as described in this scenario. The Nacha Rules do not address returns for goods that were never received so the Consumer's Bank would not be able to take advantage of any interbank process to recover the funds for the Consumer.

IV.B.3.b. The Consumer's Bank's Error Resolution Obligations

As the Consumer has not asserted an error, the Consumer's Bank does not have any error resolution obligations.

IV.B.3.c. The Transfer Provider's Error Resolution Obligations

The Funding Transaction is not unauthorized as to the Transfer Provider because it was authorized by the Consumer. As the Consumer has not asserted an error, the Transfer Provider does not have any error resolution obligations.

IV.B.3.d. Interbank Recovery Options

Even though the Consumer's Bank does not have error resolution obligations, where a Consumer asserts they never received goods and the Funding Transaction involved a debit card transaction, the Consumer's Bank may be able to charge back (i.e., return) the debit card transaction under the applicable card network rules. The card network rules permit the Consumer's Bank to initiate a chargeback of a debit card transaction for non-receipt of goods, provided any applicable conditions have been met, although charge back rights may vary when the debit card was used for the Funding Transaction (i.e., where the Transfer Provider is the merchant) and the Receiver of the Payment Transaction is the provider of goods not received.[78] If card network rules permit the chargeback, the Transfer Provider's merchant acquiring bank then must absorb the loss for the amount of the debit card transaction, unless it can show it has issued a refund or the goods were received. Typically, the Transfer Provider's bank passes through these losses and responsibilities to the Transfer Provider by contract.

IV.C. A Fraudster Associates the Consumer's Bank Account Information with the Fraudster's Transfer Provider Access Device

IV.C.1. A Fraudster Provides the Consumer's Payment Information to the Transfer Provider for Use in Funding Transactions for Intermediated Transfers Initiated through Fraudster's Transfer Provider Access Device – Baseline Scenario (Debit Card)

A fraudster obtains the Consumer's debit card information. The fraudster establishes a Prepaid Account or Wallet relationship with the Transfer Provider and uses the Consumer's debit card information as the payment method for Funding Transactions. The fraudster instructs the Transfer Provider to transfer funds and the Transfer Provider executes that instruction via an Intermediated Transfer. The Consumer's account at the Consumer's Bank is debited via the debit card information. The Consumer does not have a relationship with the Transfer Provider.

IV.C.1.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction is an unauthorized EFT as the Transfer Provider did not have "actual authority" to initiate EFTs from the Consumer's account at the Consumer's Bank. The fraudster is unable to give such authority to the Transfer Provider because the fraudster is not an accountholder authorized to transact on the Consumer's account at the Consumer's Bank, is not an authorized user of the access device issued by the Transfer Provider, or otherwise acting on behalf of the Consumer. That the fraudster gained access to the Consumer's account at the Consumer's Bank through the Transfer Provider does not impact whether the fraudster has authority to authorize EFTs from such account. The CFPB has affirmed its position that these transfers are considered unauthorized when the Consumer has no relationship with the Transfer Provider.[79] The Consumer has asserted an error to the Consumer's Bank.

IV.C.1.b. The Consumer's Bank's Error Resolution Obligations

The Consumer's Bank has full error resolution obligations for the Funding Transaction under this scenario. The Transfer Provider is not a Financial Institution with respect to the Consumer because it does not hold the Consumer's account and it has not agreed with the Consumer to provide EFT services. The Transfer Provider also is not a Service Provider

[78] The Visa rules do not specifically address charge backs for transactions involving digital wallet operators. However, the Mastercard rules state that a charge back for non-receipt of goods cannot be used for transactions involving Staged Digital Wallets when "the funds did not appear in the [Staged Digital Wallet]" and "chargeback rights are not available for any subsequent purchase of goods or service from [a Staged Digital Wallet]." Mastercard Chargeback Guide, Merchant Edition, 26 April 2022.

[79] EFT FAQs, Error Resolution: Unauthorized EFTs, Questions 3, 11.

with respect to the Consumer because it has not issued an access device to the Consumer that the Consumer can use to access the Consumer's account held by the Consumer's Bank.

IV.C.1.c. The Transfer Provider's Error Resolution Obligations

As the Transfer Provider is neither a Financial Institution nor a Service Provider with respect to the Consumer, it does not have any error resolution obligations.[80]

IV.C.1.d. Interbank Recovery Options

Where a Consumer denies authorizing or participating in the Funding Transaction, the Consumer's Bank may charge back (i.e., return) the debit card transaction under the applicable card network rules. The card network rules permit the Consumer's Bank to initiate a chargeback of a debit card transaction for fraud within 120 calendar days from the transaction date. The Transfer Provider's merchant acquiring bank then must absorb the loss for the amount of the debit card transaction, unless it can show it has issued a refund or the transaction was authorized. Typically, the Transfer Provider's bank passes through these losses and responsibilities to the Transfer Provider by contract. This process happens outside the scope of Regulation E and the Consumer's Bank's ability to charge back the transaction has no impact on its Regulation E obligations.

IV.C.2. A Fraudster Provides the Consumer's Payment Information to the Transfer Provider for Use in Funding Transactions for Intermediated Transfers Initiated through Fraudster's Transfer Provider Access Device – Scenario Variation 2 (ACH Debit)

The facts are the same as in the Baseline Scenario (IV.C.1) except the fraudster has used the Consumer's ACH information as the payment method for Funding Transactions.

IV.C.2.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction is an unauthorized EFT for the same reasons as discussed in the Baseline Scenario.

IV.C.2.b. The Consumer's Bank's Error Resolution Obligations

The Consumer's Bank will have full error resolution obligations for the Funding Transaction for the same reasons as discussed in the Baseline Scenario.

IV.C.2.c. Transfer Provider's Error Resolution Obligations

The Transfer Provider does not have any error resolution obligations for the same reasons as discussed in the Baseline Scenario.

IV.C.2.d. Interbank Recovery Options

Where a Consumer denies authorizing or participating in the Funding Transaction, the Consumer's Bank may return the ACH debit under the Nacha Rules. The Nacha Rules permit the Consumer's Bank to return an unauthorized ACH debit within 60 calendar days from the Settlement Date of the transfer if it obtains a Written Statement of Unauthorized Debit from the Consumer and credits the Consumer's account for the amount of the returned ACH debit. The Transfer Provider's bank that originated the unauthorized debit must refund the amount of that transfer to the Consumer's Bank. Typically, the Transfer Provider's bank passes through the financial loss associated with such returns to the Transfer Provider. This process happens outside the scope of Regulation E and the Consumer's Bank's ability to recover the funds through an ACH return has no impact on its Regulation E obligations.

IV.D. Misdirected Payments

IV.D.1. Misdirected Payment Due to the Transfer Provider's Token Records Error – Baseline Scenario (Debit Card)

The Consumer has a Prepaid Account or Wallet relationship with a Transfer Provider. The Consumer has provided debit card information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions. The Consumer instructs the Transfer Provider to transfer funds to Person A and the Transfer Provider executes that instruction via an Intermediated Transfer. In the instruction to the Transfer Provider, the Consumer uses the correct token information (e.g., email address or mobile phone number) to identify Person A. Due to inaccurate or outdated information in the Transfer Provider's directory, Person A's information is incorrectly associated with Person B. The funds are transferred to Person B due to the directory error.

[80] While the Transfer Provider is not required to resolve the Consumer's claim under Regulation E, the Consumer may have claims against the Transfer Provider and the fraudster under other applicable laws.

IV.D.1.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

Although "incorrect" EFTs are not defined by the EFTA or Regulation E, the CFPB has opined these types of misdirected payments may be incorrect EFTs.[81] However, the CFPB did not explain what types of "person-to-person digital payment network services" it believes are covered by this opinion on misdirected payments. As the opinion was provided in connection with supervisory examinations of institutions, the CFPB seems to be addressing only those services being offered directly by a Financial Institution (i.e., a service a bank offers to its customers in partnership with a P2P provider or a service offered by a P2P provider that is a Regulation E Financial Institution).[82] In that case, the CFPB expects the Financial Institution to ensure information related to services it offers is correct and up to date. The CFPB did not expressly address the obligations of a Financial Institution holding the account used to fund a P2P transfer where the P2P payment services are offered by third party, as is the case with Intermediated Transfers. As such, a Consumer's Bank that does not directly offer the applicable P2P services is likely outside the scope of the CFPB's opinion.

The Intermediated Transfer services here are provided by the Transfer Provider and not by the Consumer's Bank. The Consumer's Bank only has responsibility for the Funding Transaction, which does not involve an error as the incorrect directory information did not impact the execution of the Funding Transaction. Specifically, the Consumer's Bank properly processed the incoming debit to the Consumer's account, which transferred funds from the Consumer's account at the Consumer's Bank to the Transfer Provider.

Only the Transfer Provider is responsible for the misdirected Intermediated Transfer because it occurred solely as part of the Transfer Provider's responsibilities in carrying out the Consumer's instructions via the Intermediated Transfer. The Consumer's Bank can further bolster its position by showing it has no relationship with the Transfer Provider and no control over or ability to determine the accuracy of the Transfer Provider's directory.

Where there was no error in executing the Funding Transaction, the misdirected Intermediated Transfer is not an incorrect EFT with respect to the Consumer's Bank. As the Consumer initiated the Intermediated Transfer, it is not an unauthorized EFT. The Consumer's claim also does not fall within any of the other error categories discussed in Section III.A.7. The Consumer has not asserted an error to the Consumer's Bank.

IV.D.1.b. The Consumer's Bank's Error Resolution Obligations

As the Consumer has not asserted an error, the Consumer's Bank does not have any error resolution obligations.[83]

IV.D.1.c. The Transfer Provider's Error Resolution Obligations

The Intermediated Transfer is an incorrect EFT as to the Transfer Provider based on the CFPB's guidance. The Transfer Provider is a Financial Institution because it has issued an Access Device to the Consumer and agreed with the Consumer to provide EFT services through Intermediated Transfers. As the issue stems from the Transfer Provider's directory and results in the Intermediated Transfer being delivered to an unintended Receiver, any argument that the Intermediated Transfer is not an incorrect EFT will most likely be unsuccessful. As a Financial Institution with respect to the Intermediated Transfer, the Transfer Provider has full error resolution obligations.

IV.D.1.d. Interbank Recovery Options

The card network rules do not address interbank recovery for these types of misdirected payments.

IV.D.2. Misdirected Payment Due to the Transfer Provider's Token Records Error – Scenario Variation 2 (ACH Debit)

The facts are the same as in the Baseline Scenario (IV.D.1) except the Consumer has provided ACH information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions.

[81] CFPB Supervisory Highlights, Issue 25, Fall 2021, available at https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-25_2021-12.pdf. As "incorrect" EFTs are not defined in the EFTA, Regulation E, or its commentary, an informal opinion defining an incorrect EFT that occurs outside the rulemaking process is not binding law.

[82] *Id.* at page 6 ("Supervision conducted examinations of institutions in connection with the provision of person-to-person digital payment network services.").

[83] Consumer's Bank may elect to initially treat the Funding Transaction as a non-Regulation E complaint in order to investigate and confirm the misdirected payment was not in fact due to any error on Consumer Bank's part.

IV.D.2.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

The Funding Transaction is not an incorrect EFT as to the Consumer's Bank for the same reasons as discussed in the Baseline Scenario.

IV.D.2.b. The Consumer's Bank's Error Resolution Obligations

As the Consumer has not asserted an error, the Consumer's Bank does not have any error resolution obligations.

IV.D.2.c. The Transfer Provider's Error Resolution Obligations

The Intermediated Transfer is an incorrect EFT as to the Transfer Provider for the same reasons as discussed in the Baseline Scenario. As a Financial Institution with respect to the Intermediated Transfer, the Transfer Provider has full error resolution obligations. However, as the Transfer Provider is also a Service Provider, the obligations as discussed in Section III.C.1 will apply.

IV.D.2.d. Interbank Recovery Options

The Nacha Rules do not provide a returns process for the Consumer's Bank for these types of misdirected payments.

IV.D.3. Misdirected Payment Due to the Consumer's Error – Scenario Variation 3

The Consumer has a Prepaid Account or Wallet relationship with a Transfer Provider. The Consumer has provided debit card or ACH information associated with the Consumer's account at the Consumer's Bank to the Transfer Provider for use in connection with Funding Transactions. The Consumer intends to instruct the Transfer Provider to transfer funds to Person A, but, in the instruction to the Transfer Provider, the Consumer accidentally inputs incorrect identifying information. The incorrect information is associated with Person B. The Transfer Provider executes the Consumer's instruction via an Intermediated Transfer and the funds are transferred to Person B.

IV.D.3.a. The Consumer Asserts These Facts and Claims Error to the Consumer's Bank

This scenario is not directly addressed by the EFTA or Regulation E. As discussed in the baseline scenario, the CFPB's opinion suggests an incorrect EFT involves some issue or mistake caused by the Financial Institution offering a P2P payment service. There is no controlling guidance suggesting a mistake by the consumer results in an incorrect EFT. Further, the Intermediated Transfer services here are provided by the Transfer Provider and not by the Consumer's Bank. As the Consumer initiated the Intermediated Transfer, it is not an unauthorized EFT. The Consumer's claim also does not fall within any of the other error categories discussed in Section III.A.7. The Consumer has not asserted an error to the Consumer's Bank.

IV.D.3.b. The Consumer's Bank's Error Resolution Obligations

As the Consumer has not asserted an error, the Consumer's Bank does not have any error resolution obligations.

IV.D.3.c. The Transfer Provider's Error Resolution Obligations

The Intermediated Transfer is not an incorrect EFT as to the Transfer Provider as there is no applicable guidance suggesting as much. As the Consumer has not asserted an error, the Transfer Provider does not have any error resolution obligations.

IV.D.3.d. Interbank Recovery Options

Neither the card network rules nor the Nacha Rules address interbank recovery for these types of misdirected payments.

IV.E. Amount Errors

If the Transfer Provider makes a mistake in executing the Consumer's instruction to send a particular amount of funds, under Regulation E the mistake constitutes a "computational or bookkeeping error made by the financial institution [the Transfer Provider] relating to an [EFT]."[84] Thus, the Transfer Provider is responsible for resolving such amount errors in any scenario where the Transfer Provider's mistake results in a different amount of funds being debited from the Consumer's account or delivered to the Receiver than the amount the Consumer had instructed.

Under Regulation E, the "computational or bookkeeping" error category encompasses only those "error[s] made by the financial institution." Therefore, when the amount of a Funding Transaction differs from the Consumer's instruction due to a mistake by the Transfer Provider, such "computational or bookkeeping" error would not apply to

[84] 12 C.F.R. 1005.11(a)(1)(iv).

the Consumer's Bank as it did not make the mistake. In that case, the Consumer's Bank is not required to investigate and resolve the error.

However, if the Transfer Provider's mistake results in a debit to the Consumer's Account in excess of what the Consumer authorized, the Consumer's Bank is also responsible for resolving the error but only as to the excess amount. The debit of such excess amount is unauthorized and the error resolution requirements and interbank recovery options previously discussed would apply.[85]

IV.F. Funding Variations

A P2P transfer may involve an Intermediated Transfer or a Split-Funded P2P Transfer or may be fully funded by a Stored Balance.

Where a P2P transfer is wholly funded by a Stored Balance in the Consumer's Prepaid Account and the Consumer has asserted an error, only the Transfer Provider has Regulation E error resolution obligations. The Consumer's Bank does not have error resolution obligations because no part of the P2P transfer involved an EFT to the account held by the Consumer's Bank.

Where a P2P transfer is a Split-Funded P2P Transfer and the Consumer has asserted an error, both the P2P Provider and the Consumer's Bank have Regulation E error resolution obligations with respect to the portion of the transfer that is the Intermediated Transfer, but only the P2P Provider has error resolution obligations with respect to the portion of the transfer that is the Stored Balance Transfer.

For example, consider a $100 Split-Funded P2P Transfer that is funded by a $40 Stored Balance and a $60 Funding Transaction. With respect to the Funding Transaction, the P2P Provider is a Transfer Provider and therefore is a Financial Institution under Part (b) and may be a Service Provider if the Funding Transaction is made via an ACH debit. The Consumer's Bank is also a Financial Institution for the Funding Transaction as it holds the account being debited (i.e., the Consumer's account at the Consumer's Bank). However, the P2P Provider is a Financial Institution under Part (a) for the Stored Balance Transfer portion of the P2P transfer because it holds the Consumer's account that is being debited (i.e., the Consumer's Prepaid Account with the P2P Provider). The Consumer's Bank is not a Financial Institution for the Stored Balance Transfer portion because it does not hold the account being debited and has not issued an Access Device for such account. As a result, the Consumer's Bank is responsible for error resolution only as to the Funding Transaction portion of the transfer as only that portion resulted in an EFT to the account held by the Consumer's Bank (i.e., the $60 Funding Transaction). The P2P Provider is responsible for error resolution as to the full $100 Split-Funded P2P Transfer because it is a Financial Institution for the entire P2P transfer. If the P2P Provider credits the Consumer for an error involving the Split-Funded P2P Transfer, the Consumer's Bank may be able to rely on that information to show that any error specific to the Funding Transaction has been resolved and it is not also required to provide a credit for the same error, as discussed in Sections III.C.1 and III.D.1.a.

[85] This position is supported by past rulemakings discussing the provisional credit requirement, where the Board stated "[t]his section requires the institution to provisionally recredit the consumer's account in the amount of the alleged error. Some commenters requested clarification of the amount that should be recredited if only part of the transfer is questioned. If the statement reflects a $100 transfer and the consumer claims to have made a $10 transfer, for example, the institution would have to recredit $90, not $100." Electronic Fund Transfers, 45 Fed. Reg. 8255 (Feb. 6, 1980). Although the Board did not opine on what type of error this would be, the excess amount would likely be considered unauthorized from the Consumer's Bank's perspective as the Transfer Provider did not have authority to debit the excess amount.

V. Card Network Chargeback Disputes

Under the payment card network rules,[86] the Sender's Bank may be able to charge back a debit card transaction to the Transfer Provider's merchant acquiring bank. Where the Sender's Bank is liable to the Sender for a transaction, the chargeback process potentially allows the Sender's Bank to shift the loss to the Transfer Provider's merchant acquiring bank, who will typically pass the loss on to the Transfer Provider. The Sender's Bank is not required to have suffered a loss in order to take advantage of the chargeback process as the process happens completely outside the scope of any party's Regulation E obligations or liabilities. The types of disputes covered by the chargeback process are broader than those covered by Regulation E's error resolution process. In other words, even if a Sender's dispute is not covered by Regulation E, it may be covered by the chargeback process.

The chargeback process typically begins when the Sender notifies the Sender's Bank of a dispute regarding a debit card transaction, such as by claiming the transaction is unauthorized or that they never received the goods or services paid for with the transaction. Once the Sender's Bank has sufficient information regarding a transaction, it may initiate a chargeback, even if the Sender has not specifically asked the Sender's Bank to do so. Depending on the type of dispute involved, the Sender's Bank may be required to certify or provide documentation supporting the Sender's dispute as part of the chargeback process or the Sender may be required to take certain actions before being able to take advantage of the chargeback process. The Sender's Bank may also be required to provide a provisional credit to the Sender as part of the chargeback process.

Once the Sender's Bank submits a chargeback claim, the acquiring bank typically has an opportunity to represent the charge (i.e., dispute the chargeback). For example, when the Sender's Bank charges back a debit card transaction because the Sender denies authorizing or participating in the transaction, the acquiring bank may be able to represent the charge if it has evidence that the Sender authorized the transaction or the dispute is invalid. If an acquiring bank represents a charge, the Sender's Bank may either accept the representment or continue to dispute the transaction. If the Sender's Bank accepts the representment, liability for the transaction shifts back to the Sender's Bank. If the Sender's Bank decides to continue to dispute the transaction, it may either submit a second chargeback (such as if it has new evidence) or it may be subject to an arbitration claim from the acquiring bank or the Transfer Provider.

Consider a scenario where a Sender has claimed they did not authorize a Funding Transaction conducted via a debit card transaction. The Sender's Bank initiates a chargeback to the Transfer Provider's merchant acquiring bank and provides provisional credit to the Sender. The acquiring bank notifies the Transfer Provider that the Funding Transaction has been charged back. Upon notice of the chargeback, the Transfer Provider collects sufficient evidence[87] that the Sender authorized the transaction and provides that evidence to its acquiring bank. The acquiring bank provides the evidence to the Sender's Bank through a representment. After reviewing the evidence, the Sender's Bank must determine whether to accept or deny the representment.

If the Sender's Bank decides to continue to dispute the transaction, either by rejecting the representment or submitting a second chargeback, the Transfer Provider can also continue to dispute the chargeback and the parties may end up in arbitration. The arbitration process is also governed by the applicable card network rules.

As the Transfer Provider can dispute a chargeback, the chargeback process is not a guarantee of recovery for the Sender's Bank. As a result, the Sender's Bank may still be liable for any loss even after it goes through the chargeback process.

[86] This section provides a general overview of the chargeback process. However, the specific requirements and processes may vary based on the type of dispute involved and the applicable payment network rules.

[87] Depending on the applicable card network rules, this evidence may include documentation that the transaction was initiated using the Sender's mobile device or other documentation showing a link between the Sender and the transaction.

VI. Conclusion

As P2P transfers continue to be popular with consumers, understanding each party's obligations for error resolution when the P2P payment service uses Intermediated Transfers is important for all parties involved. This helps ensure consumers know which party they should reach out to when there are unauthorized payments or other errors involving an Intermediated Transfer. Transfer Providers that offer EFT services play a key role in protecting their consumer customers and should understand the scope of their Regulation E responsibilities. It is also important for banks to understand their regulatory obligations even though Intermediated Transfers are offered and facilitated by a Transfer Provider. Clarity for all parties involved ensures consumer's error claims are investigated and resolved by the applicable financial institution in a compliant and timely manner.

Appendix A

This Appendix A provides additional details on the procedures a Financial Institution must follow in connection with fulfilling its error resolution obligations.

1. Consumer's Notice of Error

A consumer's notice of error may be either oral or written. If a consumer provides oral notice, the Financial Institution may require the consumer to provide written confirmation of the error within 10 days of the oral notice, but the timing requirements are still based on the date the Financial Institution received the oral notice.[88] If the Financial Institution requires such written confirmation, it must inform the consumer of the requirement and where the confirmation must be sent at the time the consumer provides oral notice.[89]

Financial Institutions may require the consumer to give notice only at a specified telephone number or address disclosed by the Financial Institution as long as the Financial Institution "maintains reasonable procedures to refer the consumer to the specified telephone number or address if the consumer attempts to give notice to the institution in a different manner."[90] If the Financial Institution maintains such procedures and those procedures were followed with respect to a consumer, then the Financial Institution is not obligated to act on a notice of error provided to the wrong address by that consumer.

2. Required Scope of Investigation

A Financial Institution must review its own records for each alleged error.[91] If the error involved a transfer to or from a third party, a Financial Institution's review of its own records satisfies the investigation requirements if the Financial Institution does not have an agreement with the third party for the type of EFT involved.[92] An "agreement" for purposes of the investigation requirements includes any "agreement that a third party will honor an access device."[93] Participation in transfers "that are cleared through an ACH or similar arrangement for the clearing and settlement of fund transfers generally" does not constitute an agreement, even if the Financial Institution "agrees to be bound by the rules of such an arrangement."[94]

If there is no agreement between the Financial Institution and the third party, a Financial Institution "must review any relevant information within the institution's own records for the particular account to resolve the consumer's claim. The extent of 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. Information that may be reviewed as part of an investigation might include:

- The ACH transaction records for the transfer;
- The transaction history of the particular account for a reasonable period of time immediately preceding the allegation of error;
- Whether the check number of the transaction in question is notably out-of-sequence;
- The location of either the transaction or the payee in question relative to the consumer's place of residence and habitual transaction area;
- Information relative to the account in question 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; or
- Any other information appropriate to resolve the claim."[95]

If there is an agreement between the Financial Institution and the third party, a Financial Institution's review of only its own

[88] 12 C.F.R. § 1005.11(b)(2).

[89] *Id.*

[90] 12 C.F.R. Part 1005, Supp. I, comment 11(b)(1)-6.

[91] 12 C.F.R. § 1005.11(c)(4).

[92] *Id.*

[93] 12 C.F.R. Part 1005, Supp. I, comment 11(c)(4)-4.

[94] *Id.*

[95] 12 C.F.R. Part 1005, Supp. I, comment 11(c)(4)-5.

records may not satisfy the investigation requirements. "[I]f a merchant honors an access device in a shared system and a consumer asserts an error involving that transfer, for example, the financial institution must check with the merchant."[96] In such cases, review of the Financial Institution's own records should be supplemented by information supplied by the merchant unless the Financial Institution is able to definitively determine that no error occurred based on its own records.[97] A Financial Institution is permitted to correct an error without conducting an investigation, provided it complies with all other applicable error resolution requirements.[98]

A Financial Institution has 10 business days to complete the investigation and determine whether an error has occurred.[99] The 10 business-day timeframe can be extended to 45 calendar days if the Financial Institution does the following:

- Provisionally credits the consumer's account in the amount of the alleged error within 10 business days of receiving the consumer's error notice;
- Informs the consumer of the amount and date of the provisional credit within two business days of making such credit; and
- Allows the consumer full use of the provisionally credited funds.[100]

If a Financial Institution required written confirmation of an oral notice and did not receive such confirmation within 10 business days of the oral notice, the Financial Institution does not have to provide the provisional credit but may still take advantage of the 45-day timeframe.[101] If the error involves an alleged unauthorized EFT and the Financial Institution has complied with the liability provisions discussed in paragraph 4 below, the Financial Institution may withhold a maximum of $50 from the provisional credit.[102]

The 45-day timeframe may also be extended further in certain situations. A Financial Institution may take up to 90 calendar days to complete its investigation when the EFT at issue resulted from a point-of-sale debit card transaction.[103] This includes all debit card transactions made at a merchants' point-of-sale terminal, including cash-only, mail and telephone transactions.[104] A 90-day timeframe also applies when the EFT at issue was not initiated in a state.[105] A special timeframe also applies when the EFT at issue was made within thirty days after the first deposit to the account. In that case, the original 10 business-day timeframe is automatically extended to 20 business days and the 45-day timeframe is automatically extended to 90 calendar days.[106]

3. Determination Whether Error Occurred

After completing the investigation, a Financial Institution has three business days to notify the consumer of the results.[107] If the investigation reveals that an error occurred, the Financial Institution must correct the error within one business day after determining an error occurred.[108] The correction must include crediting interest and refunding fees, if applicable.[109] Notice to the consumer that the error occurred as alleged may be provided either in writing or orally.[110] If investigation reveals that no error occurred or a different error occurred, the Financial Institution must provide a written explanation

[96] 45 Fed. Reg. 8256.

[97] See Green v. Capital One, N.A., 557 F. Supp. 3d 441, 452-453 (S.D.N.Y. 2021) ("Capital One cites [Cifaldo v. BNY Mellon Inv. Serv. Trust Co.] to argue that its outreach to Square fulfilled its statutory obligations. In Cifaldo, the District of Nevada found the defendant had "sufficiently investigated" the alleged error under § 1693f when the defendant's letter stated that its denial "was based on the information provided to [it] verbally by the merchant," and subsequently provided the plaintiff with documentation corroborating the merchant's verbal representations. . . . [Section] 205.11 and the Official Interpretation make clear that a financial institution's core obligation is to conduct a reasonable investigation of its own records, and that outreach to a third-party merchant is simply one permissible investigative technique to supplement such an investigation. . . . Thus, with due consideration of the Official Interpretation, Cifaldo is best understood as holding that a third-party merchant's evidence and representation that a transaction was authorized may suffice to meet § 1693f's investigatory requirements—such as when the plaintiff fails to allege that there is other relevant evidence within the bank's own records that the bank failed to consider—but it does not constitute a per se rule.")

[98] 12 C.F.R. Part 1005, Supp. I, comment 11(c)-4.

[99] 12 C.F.R. § 1005.11(c)(1).

[100] 12 C.F.R. § 1005.11(c)(2).

[101] 12 C.F.R. § 1005.11(c)(2)(i)(A).

[102] 12 C.F.R. § 1005.11(c)(2)(i).

[103] 12 C.F.R. § 1005.11(c)(3)(ii)(B).

[104] 12 C.F.R. Part 1005, Supp. I, comment 11(c)(3)-1.

[105] 12 C.F.R. § 1005.11(c)(3)(ii)(A).

[106] 12 C.F.R. § 1005.11(c)(3)(i), (c)(3)(ii)(C).

[107] 12 C.F.R. § 1005.11(c)(1), (c)(2)(iv).

[108] 12 C.F.R. § 1005.11(c)(1), (c)(2)(iii).

[109] 12 C.F.R. Part 1005, Supp. I, comment 11(c)-6.

[110] 12 C.F.R. Part 1005, Supp. I, comment 11(c)-1.

of its findings to the consumer, including a statement that the consumer has a right to request the documentation supporting that finding.[111] Documentation must be provided promptly upon such a request.[112]

If a Financial Institution will debit a provisional credit, it must notify the consumer of the following: (i) the date of the debit; (ii) the amount of the debit, and (iii) that the Financial Institution will honor, without charge, all checks, drafts, or similar instruments payable to third parties and preauthorized transfers from the account for five business days after the notification. [113] A Financial Institution only needs to honor items that would have been paid if the provisional credit had not been debited.[114] As an alternative to honoring items for five business days, a Financial Institution may notify the consumer that their account will be debited five business days from the notice, specifying the calendar date on which the account will be debited.[115]

4. Consumer Liability for Error

If the error involves an unauthorized EFT, the Financial Institution may impose some liability on the consumer under certain circumstances. As a prerequisite to imposing liability, the Financial Institution must disclose to the consumer a summary of consumer's liability for an unauthorized EFT, the telephone number and address where a consumer may notify the Financial Institution of an unauthorized EFT, and the Financial Institution's business days.[116] If an access device was used as part of the unauthorized EFT, two additional prerequisites apply: (i) it must be an accepted access device[117] and (ii) the Financial Institution must have provided a way to identify the consumer to whom the device was issued, such as a PIN or signature comparison.[118]

The amount of liability a Financial Institution may impose on a consumer depends on when the consumer notifies the Financial Institution that an unauthorized EFT has occurred. Notice may be provided in person, by telephone, or in writing and is considered given when the consumer takes reasonable steps to provide the Financial Institution with pertinent information, regardless of whether the Financial Institution actually receives such notice.[119] Where the Financial Institution has disclosed a specific telephone number or address for consumers to provide notice of an unauthorized EFT and the consumer provides notice at a different telephone number or address, the Financial Institution is still considered to have received the notice.[120] A Financial Institution may also receive constructive notice, such as when the Financial Institution on its own learns of information sufficient to lead to a reasonable belief that an unauthorized EFT has occurred.[121]

[111] 12 C.F.R. § 1005.11(d)(1).

[112] *Id.*

[113] 12 C.F.R. § 1005.11(d)(2).

[114] 12 C.F.R. § 1005.11(d)(2)(ii).

[115] 12 C.F.R. Part 1005, Supp. I, comment 11(d)(2)-1.

[116] 12 C.F.R. § 1005.6(a).

[117] "An access device becomes an 'accepted access device' when the consumer: (i) Requests and receives, or signs, or uses (or authorizes another to use) the access device to transfer money between accounts or to obtain money, property, or services; (ii) Requests validation of an access device issued on an unsolicited basis; or (iii) Receives an access device in renewal of, or in substitution for, an accepted access device from either the financial institution that initially issued the device or a successor." 12 C.F.R. § 1005.2(a)(2).

[118] 12 C.F.R. § 1005.6(a); 12 C.F.R. Part 1005, Supp. I, comment 6(a)-1.

[119] 12 C.F.R. § 1005.6(b)(5).

[120] 12 C.F.R. Part 1005, Supp. I, comment 6(b)(5)-1.

[121] 12 C.F.R. § 1005.6(b)(5)(iii).

The timeframes for providing notice depend on whether or not an Access Device was used. If an Access Device used in an alleged unauthorized EFT was lost or stolen, there are three tiers of consumer liability, and the applicable tier is determined based on the timeframe within which the consumer provides notice to the Financial Institution that the Access Device was lost or stolen:

	Tier 1	Tier 2	Tier 3
Timeframe	Unauthorized EFTs occurring within two business days from the date the consumer learns of the loss or theft.[122]	Unauthorized EFTs occurring more than two business days after the consumer learns of the loss or theft but within 60 calendar days of the date the Financial Institution sends the periodic statement reflecting the first unauthorized EFT.[123]	Unauthorized EFTs occurring more than 60 calendar days from the date the Financial Institution sends the periodic statement reflecting the first unauthorized EFT.[124]
Liability Calculation	The amount of the unauthorized EFTs occurring within the Tier 1 timeframe, up to $50.[125]	Tier 1 amount plus amount of the unauthorized EFTs occurring within the Tier 2 timeframe, up to $500.[126]	Tier 2 amount plus amount of the unauthorized EFTs occurring within the Tier 3 timeframe.[127]

The consumer is not liable for unauthorized EFTs occurring after notice is provided to the Financial Institution. For example, if the consumer provides notice during the Tier 2 timeframe, the liability calculation runs through the notice date rather than through the full Tier 2 timeframe.

If no Access Device was used, or if an Access Device was used but was not lost or stolen, there are two tiers of liability which are based on the timeframe within which the consumer provides notice to the Financial Institution of the unauthorized EFTs:

	Tier 1	Tier 2
Timeframe	Unauthorized EFTs occurring within 60 days of the date the Financial Institution sends the periodic statement reflecting the first unauthorized EFT.[128]	Unauthorized EFTs occurring more than 60 days from the date the Financial Institution sends the periodic statement reflecting the first unauthorized EFT.[129]
Liability Calculation	No liability.[130]	Amount of the unauthorized EFTs occurring within the Tier 2 timeframe.[131]

[122] 12 C.F.R. § 1005.6(b)(1). The day the consumer learns of the loss or theft does not count towards the two business days. 12 C.F.R. Part 1005, Supp. I, comment 6(b)(1)-3.

[123] 12 C.F.R. § 1005.6(b)(2).

[124] 12 C.F.R. § 1005.6(b)(3).

[125] 12 C.F.R. § 1005.6(b)(1); 12 C.F.R. Part 1005, Supp. I, comment 6(b)(1)-1.

[126] 12 C.F.R. § 1005.6(b)(2); 12 C.F.R. Part 1005, Supp. I, comment 6(b)(2)-1. In order to impose liability for unauthorized EFTs occurring after the Tier 1 timeframe, the Financial Institution must be able to show the unauthorized EFTs would not have occurred had the consumer provided notice within the Tier 1 timeframe.

[127] 12 C.F.R. § 1005.6(b)(2); 12 C.F.R. Part 1005, Supp. I, comment 6(b)(3)-1. In order to impose liability for unauthorized EFTs occurring after the Tier 2 timeframe, the Financial Institution must be able to show the unauthorized EFTs would not have occurred had the consumer provided notice within the Tier 2 timeframe.

[128] 12 C.F.R. § 1005.6(b)(3).

[129] *Id.*

[130] 12 C.F.R. § 1005.6(b)(3); 12 C.F.R. Part 1005, Supp. I, comment 6(b)(3)-2.

[131] 12 C.F.R. § 1005.6(b)(3); 12 C.F.R. Part 1005, Supp. I, comment 6(b)(3)-2. In order to impose liability for unauthorized EFTs occurring after the Tier 1 timeframe, the Financial Institution must be able to show the unauthorized EFTs would not have occurred had the consumer provided notice within the Tier 1 timeframe.

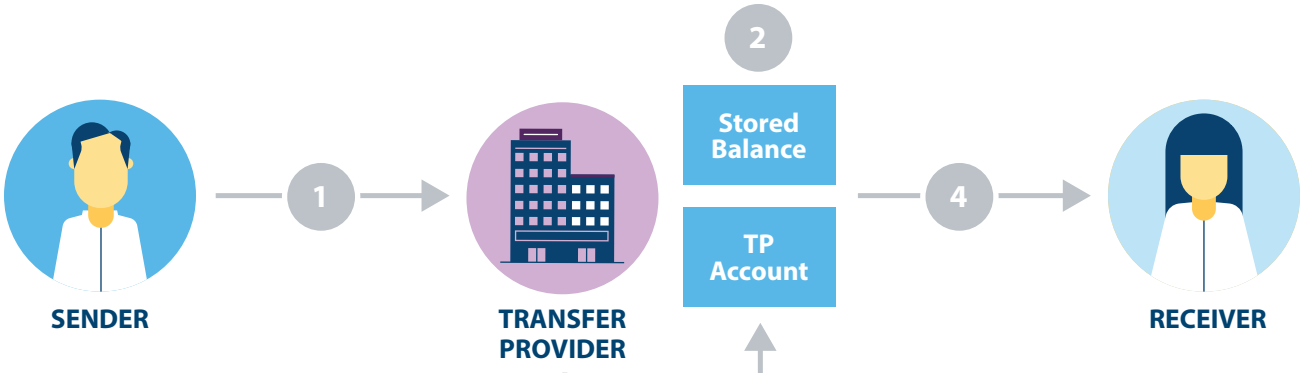
The consumer is not liable for unauthorized EFTs occurring after notice is provided to the Financial Institution. For example, if the consumer provides notice during the Tier 2 timeframe, the liability calculation runs through the notice date and the consumer cannot be held liable for unauthorized EFTs occurring after the notice date.

If a Financial Institution seeks to impose liability on a consumer for an alleged unauthorized EFT, it is up to the Financial Institution to prove the EFT was authorized or the prerequisites of liability have been met.[132] As a result, if a Financial Institution seeks to conclude that an alleged unauthorized EFT was authorized (i.e., that no error occurred), then the Financial Institution has the burden of collecting sufficient evidence to prove the consumer authorized the EFT at issue. Similarly, if a Financial Institution seeks to impose liability on the consumer for unauthorized EFTs, then the Financial Institution has the burden of showing it complied with the applicable prerequisites.

[132] 15 U.S.C. § 1693g(b).

Appendix B

Split-Funded P2P Transfer Example Illustration

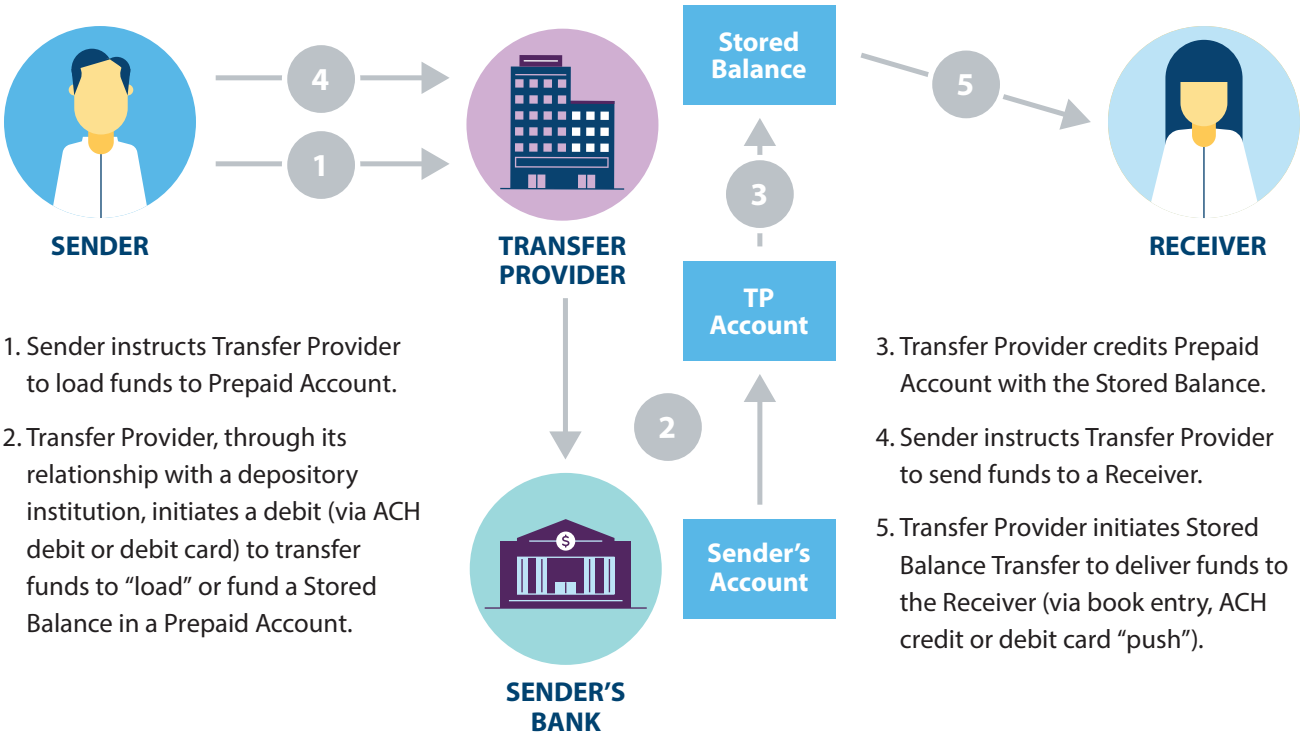


1. Sender instructs Transfer Provider to pay Receiver.
2. Sender has a stored balance in a Prepaid Account with the Transfer Provider that will cover some but not all of the payment amount.
3. Transfer Provider, through its relationship with a depository institution, initiates a Funding Transaction (via ACH debit or debit card) to transfer funds to the TP Account for the remainder of the payment amount.
4. Transfer Provider initiates Split-Funded P2P Transfer to deliver funds to the Receiver (via book entry, ACH credit or debit card "push"). The portion of a Split-Funded P2P Transfer that is funded by a Funding Transaction is an Intermediated Transfer; the portion of a Split-Funded P2P Transfer that is funded by a Stored Balance is a Stored Balance Transfer.

Notes:

- For simplicity, the illustration does not reflect the Transfer Provider's bank, which at the Transfer Provider's direction would originate/transmit the Funding Transaction into the ACH network or card network. The same bank may also hold the TP Account for the Transfer Provider.

Stored Balance Transfer Example Illustration



1. Sender instructs Transfer Provider to load funds to Prepaid Account.
2. Transfer Provider, through its relationship with a depository institution, initiates a debit (via ACH debit or debit card) to transfer funds to "load" or fund a Stored Balance in a Prepaid Account.
3. Transfer Provider credits Prepaid Account with the Stored Balance.
4. Sender instructs Transfer Provider to send funds to a Receiver.
5. Transfer Provider initiates Stored Balance Transfer to deliver funds to the Receiver (via book entry, ACH credit or debit card "push").

Notes:

- For simplicity, the illustration does not reflect the Transfer Provider's bank, which at the Transfer Provider's direction would originate/transmit the debit into the ACH network or card network. The same bank may also hold the TP Account for the Transfer Provider.