

# What Is An EFT Payment?

Written By

**E. Napoletano** Contributor **Mitch Strohm**

**Fact Checked**

Updated: Jun 29, 2022, 1:36pm

An electronic funds transfer (EFT) is a way to move money across an online network, between banks and people. EFT payments are frequently used in place of paper-based payment methods—like checks and cash—to make transactions faster and safer.

When you make a payment these days, odds are you're using an EFT to make it happen. Friends can use EFT payments to split a restaurant bill, and businesses can use EFT payment options to get paid by their customers. With so many uses, EFT payments are essential to how money moves through the economy and your life.

## What Is an Electronic Funds Transfer?

An electronic funds transfer is the electronic transfer of money between people, banks and companies. This payment technology is used to pay bills, send money to friends and family and compensate workers each payday.

---

EFT payments are a speedier alternative to physical payment methods like cash and checks. Direct deposit, credit card transactions, ATM transactions, electronic checks and phone payments are all types of EFT payments.

## What Is an EFT Payment?

An EFT payment is another name for an EFT transfer. If you've used online banking to move money from your checking to your savings account, you've used EFT technology. Likewise, if you've used an app on your smartphone to send money to a friend for a restaurant tab, you've used EFT technology.

## What Are Peer-to-Peer Electronic Payments?

---

Apps like Cash App, PayPal and Venmo make it easy to send funds from person to person in a flash. These peer-to-peer (P2P) payment systems use EFT technology to move money.

When you register to use one of these applications, you can link your debit card, bank account, or both. Some apps allow you to connect your credit card (usually for a charge per transaction). When you want to send a payment, you open the app, enter the information for the receiving party, confirm your transaction and send money.

P2P platforms can act as holding tanks for funds received. Some users don't transfer funds through these apps to their banks. They leave money in the app and pay vendors and people directly, using the P2P platform as a makeshift bank account. Some peer-to-peer payment apps, such as PayPal, offer debit cards to their users, making it easier to access funds held in the payment platform.

## How Does EFT Work?

---

EFT payments need two parties to work: a sender and a receiver. When the sender commits to sending funds to the receiver, that payment goes out through the appropriate payment network and moves money from the sender's account to the receiver's account.

Here are two examples to help you understand how money moves across payment networks.

1. Let's say you're at the grocery store and ready to pay. At checkout, you slide your debit card into the payment terminal to settle your bill. Once you enter your PIN and approve the transaction, money is moved in real time from your checking account to the grocery store's account. You can grab your groceries and head home.
2. Another example is a paycheck direct-deposited into your checking account. For this transaction, your employer is the sender and you're the receiver. When you set up direct deposit, you provide your employer with your bank account and routing number. Your employer inputs your banking information into their payroll provider's system. The payroll provider then initiates a transaction that debit's your employer's bank account and sends funds directly to your account. These transactions happen over the ACH network and take a few days to complete.

## What Are the Types of EFT Payments?

---

In 1978, the U.S. government passed the Electronic Fund Transfer Act (EFTA), which outlined consumer protections around specific types of electronic conveyances of money. Here are the EFT payment types protected by the EFTA:

## **Electronic Checks**

This EFT payment type replaces paper checks. Typically, you'll tell a vendor it's okay to use your checking account information to create a virtual check and submit it for payment.

## **Direct Deposit**

Instead of receiving a monthly physical check, this EFT payment method electronically deposits your payroll funds into your bank account.

## **Phone Payments**

You can pay bills over the phone by giving a company your banking information. The company then initiates a debit to your bank account for the agreed-upon amount.

## **ATM Transactions**

When you withdraw or deposit money from your accounts or move money between accounts at an ATM, you're using an EFT payment method.

## **Credit Card Transactions**

You can make payments toward your credit card balances using EFT payments. You can also use EFT to transfer balances from one credit card to another.

## **What Are the Benefits of EFT?**

---

Electronic funds transfers allow you to send and receive money faster than you would with a check.

And EFT technology makes it easy to do business where you want. You can buy groceries from your living room and tip your Uber or Lyft driver from your mobile device. You can put all of your household bills on auto-pay each month, avoiding late charges. You can pay friends, family and colleagues quickly and efficiently by using a peer-to-peer payment app.

## **Are EFT Payments Risky?**

---

At first blush, it may seem daunting to share your bank account information with a business and let it debit your account each month. The good news is that EFT payments are protected through the

Electronic Fund Transfer Act, giving you legal recourse if something's amiss with a particular transaction.

Here are some of the protections consumers enjoy under the EFTA:

- **Unauthorized transactions.** Consumers have 60 days to report any unauthorized transactions to their financial institutions for investigation. However, if you miss the 60-day window, your financial institution isn't obligated to investigate the incident.
- **Lost or stolen debit cards.** If you report your lost or stolen debit card within two days, the EFTA limits your liability for unauthorized transactions to \$50. However, if you don't report the loss or theft within 60 days, you could be liable for all unauthorized transactions.
- **Compensation for violations.** If your bank violates the guidelines established by the EFTA, you can potentially recoup damages from your bank in court.
- **Withdrawal limits.** Your bank is required to put daily withdrawal limits on your debit card to protect you from excessive and potentially unauthorized withdrawals.

It's important to note that timeliness is a key factor in limiting your liability for unauthorized transactions. It's imperative to review your bank statements regularly to check for transactions you don't recognize. You also can set up alerts with your bank—sent via text and email—that can help draw attention to transactions that aren't authorized.

## What's the Difference Between EFT and ACH?

---

ACH transactions happen on an electronic funds transfer network called the Automated Clearing House. All ACH payments are EFT payments, but not all EFT payments are ACH payments. An ACH payment must pass through the Automated Clearing House network.

ACH payments are typically used for direct payments like payroll direct deposits and recurring payments you make each month to companies for your utilities and rent. Unlike debit and credit card EFT transactions that happen in real time, ACH payments are processed in batches each day and can take one to four days to complete. Larger banks can often process ACH payments faster than smaller banks.

## Bottom Line

Electronic fund transfers facilitate the quick and safe movement of money electronically. Still, be cautious with digital payments. Be vigilant when conducting an electronic financial transaction.

Protect your PIN and only use apps you trust to send and receive money. Review your bank and credit card statements regularly to catch potential fraud early and limit your liability.



# Electronic Fund Transfers FAQs

The questions and answers below pertain to compliance with the Electronic Fund Transfer Act (EFTA) and Subpart A to Regulation E.

## Coverage: Transactions

### QUESTION 1:

What transactions are covered by the Electronic Fund Transfer Act and Regulation E?

### ANSWER (UPDATED 12/13/2021):

The Electronic Fund Transfer Act (EFTA) and Regulation E apply to an electronic fund transfer that authorizes a financial institution to debit or credit a consumer's account. 12 CFR 1005.3(a).

The term account means 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. 12 CFR 1005.2(b)(1). It includes a prepaid account, as defined by Regulation E. 12 CFR 1005.2(b)(3).

The term “electronic fund transfer” or “EFT” means 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. 12 CFR 1005.3(b)(1). Accordingly, Regulation E applies to any person-to-person (P2P) or mobile payment transactions that meet the definition of EFT, including debit card, ACH, prepaid

---

This is a Compliance Aid issued by the Consumer Financial Protection Bureau. The Bureau published a Policy Statement on Compliance Aids, available at <https://www.consumerfinance.gov/policycompliance/rulemaking/final-rules/policy-statement-compliance-aids/>, that explains the Bureau's approach to Compliance Aids.

account, and other electronic transfers to or from a consumer account. 12 CFR 1005.3(b)(1)(v); Comment 3(b)(1)-1.ii.

**QUESTION 2:**

Can person-to-person or “P2P” payments be EFTs under Regulation E?

**ANSWER** (UPDATED 12/13/2021):

Yes.

Person-to-person or “P2P” payments allow a consumer to send money to another person without needing to write a check, swipe a physical card, or exchange cash. Depending on the payment provider, a P2P payment can be initiated from a consumer’s online bank account portal, prepaid account portal, or mobile application.

Any P2P payment that meets the definition of EFT is covered by EFTA and Regulation E. See [Electronic Fund Transfers Coverage: Transactions Question 1](#) for more information about the definition of an EFT. See [Electronic Fund Transfers Coverage: Financial Institutions Question 2](#) for more information about EFTA and Regulation E’s coverage of P2P payment providers.

**QUESTION 3:**

Is a P2P payment that uses the consumer’s debit card to transfer funds considered an EFT?

**ANSWER** (UPDATED 12/13/2021):

Yes. As discussed in [Electronic Fund Transfers Coverage: Transactions Question 1](#), Regulation E applies to an EFT that authorizes a financial institution to debit or credit a consumer's account. 12 CFR 1005.3(a). The term EFT includes debit card transactions. 12 CFR 1005.3(b)(1)(v).

**QUESTION 4:**

Is a credit-push P2P payment that transfers funds out of a consumer’s deposit, prepaid, or mobile account considered an EFT?

**ANSWER** (UPDATED 12/13/2021):

Yes. As discussed in [Electronic Fund Transfers Coverage: Transactions Question 1](#), Regulation E applies to any EFT that authorizes a financial institution to debit or credit a consumer's account. 12 CFR 1005.3(a). The term EFT means 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. 12 CFR 1005.3(b)(1). A credit-push P2P payment is considered a transfer initiated through an electronic terminal, telephone, or computer for the purpose of ordering, instructing, or authorizing a financial institution to debit a consumer's account, and accordingly is an EFT.

A credit-push P2P transfer is considered an EFT even if the payment was initiated by a third party that fraudulently obtained access to consumer's account, such as by using login credentials stolen in a data breach or obtained through fraudulent inducement. In these cases, the credit-push P2P transfer would be considered an unauthorized EFT. See [Electronic Fund Transfers Error Resolution: Unauthorized EFTs Question 1](#) for more information on the definition of an unauthorized EFT.

#### **QUESTION 5:**

Is a P2P debit card “pass-through” payment considered an EFT?

**ANSWER** (UPDATED 12/13/2021):

Yes.

Generally, a “pass-through” payment transfers funds from the consumer's account held by an external financial institution to another person's account held by an external financial institution. A “pass-through” payment is initiated through a financial institution that does not hold a consumer's account, for example, a non-bank P2P provider. As discussed in [Electronic Fund Transfers Coverage: Transactions Question 1](#), Regulation E applies to any EFT that authorizes a financial institution to debit or credit a consumer's account. 12 CFR 1005.3(a). As discussed in [Electronic Fund Transfers Coverage: Transactions Question 3](#), the term EFT includes debit card transactions, and therefore debit card “pass through” payments are EFTs. 12 CFR 1005.3(b)(1)(v). See [Electronic Fund Transfers Coverage: Financial Institutions Questions 3](#) and [4](#) for more information on the error resolution obligations of the financial institutions involved in a debit card pass-through payment.



## Coverage: Financial Institutions

### QUESTION 1:

What is a financial institution under EFTA and Regulation E?

### ANSWER (UPDATED 12/13/2021):

Regulation E section 1005.2(i) defines financial institution under EFTA and Regulation E to include banks, savings associations, credit unions, and:

- any other person that directly or indirectly holds an account belonging to a consumer, or
- any other person that issues an access device and agrees with a consumer to provide electronic fund transfer (EFT) services.

12 CFR 1005.2(i).

Financial institutions include providers of P2P payment and bill payment services, if they directly or indirectly hold an account belonging to a consumer, or if they issue an access device and agree with a consumer to provide EFT services. The term financial institution does not include those excluded from coverage under section 1029 of the Dodd Frank Act. 12 CFR 1005.2(i).

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, with limited exceptions. 12 CFR 1005.11. See [Electronic Fund Transfers Error Resolution Question 2](#) for more information about these error resolution obligations.

In narrow circumstances, a financial institution can also be considered a “service provider” under Regulation E. A financial institution who provides EFT services to a consumer but does not hold the consumer’s account is a service provider under Regulation E if the financial institution: (1) issues an access device that the consumer can use to access the account and (2) no agreement exists between the access device-issuing financial institution and the account-holding financial institution. 12 CFR 1005.14(a). The automated clearing house (ACH) rules alone do not generally constitute an agreement for purposes of whether a financial institution meets the definition of “service provider” under Regulation E. However, an ACH agreement combined with another agreement to process payment transfers – such as an ACH agreement under which members specifically agree to honor each other's debit cards – is an “agreement,” and thus section 1005.14 does not apply. Comment 14(a)-2.

**QUESTION 2:**

Can non-bank P2P payment providers be considered financial institutions under Regulation E?

**ANSWER** (UPDATED 12/13/2021):

Generally, yes.

Any P2P payment provider that meets the definition of a financial institution, as discussed in [Electronic Fund Transfers Coverage: Financial Institutions Question 1](#), is a financial institution under Regulation E. Thus, if a P2P payment provider directly or indirectly holds an account belonging to a consumer, they are considered a financial institution under Regulation E. 12 CFR 1005.2(i). An example of an account that a non-bank P2P payment provider may directly or indirectly hold is a prepaid or mobile account whose primary function is to conduct P2P transfers. 12 CFR 1005.2(b)(3); Comment 2(b)(3)(i)-10. Additionally, as discussed in [Electronic Fund Transfers Coverage: Financial Institutions Question 1](#), non-account-holding providers of P2P payment or bill payment services are considered covered financial institutions under Regulation E if the provider issues an access device and agrees with a consumer to provide EFT services. 12 CFR 1005.2(i). For example, a P2P 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.

Any entity defined as a financial institution under Regulation E has error resolution obligations in the event that a consumer notifies the financial institution of an error, with limited exceptions. 12 CFR 1005.11. See [Electronic Fund Transfers Error Resolution Question 2](#) for more information about these error resolution obligations.

**QUESTION 3:**

If a non-bank P2P payment provider initiates a debit card “pass-through” payment from the consumer’s account held by a depository institution to a different person’s account at another institution, is the non-bank P2P payment provider considered a financial institution under Regulation E?

**ANSWER** (UPDATED 12/13/2021):

Generally, yes.

As discussed in [Electronic Fund Transfers Coverage: Financial Institution Question 1](#), an entity that issues an access device and agrees with a consumer to provide EFT services, is

considered a financial institution under Regulation E. As discussed in [Electronic Fund Transfers Coverage: Transactions Questions 1](#) and [5](#) a debit card “pass-through” payment is considered an EFT under Regulation E. Thus, if an entity, including a non-bank P2P payment provider, enters into an agreement with a consumer to provide EFT services and issues an access device, and initiates a debit card “pass-through” payment, then that entity would be covered as a financial institution under Regulation E. Any entity defined as a financial institution under Regulation E has error resolution obligations in the event that a consumer notifies the financial institution of an error. 12 CFR 1005.11. See [Electronic Fund Transfers Error Resolution Question 2](#) for more information about these error resolution obligations.

**QUESTION 4:**

If a consumer uses a non-bank P2P payment provider to initiate a debit card “pass-through” payment from the consumer’s account held by a depository institution, is the depository institution considered a financial institution under Regulation E, even though the transfer was initiated through the non-bank P2P payment provider?

**ANSWER** (UPDATED 12/13/2021):

Yes. As discussed in [Electronic Fund Transfers Coverage: Financial Institutions Question 1](#), the definition of financial institution includes a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide EFT services. 12 CFR 1005.2(i). Here, because the depository institution holds the consumer’s deposit account, it is considered a financial institution under Regulation E with full error resolution obligations. 12 CFR 1005.11. See [Electronic Fund Transfers Error Resolution Question 2](#) for more information about these error resolution obligations.

[Electronic Fund Transfers Coverage: Financial Institution Question 1](#) discusses a narrow circumstance where a non-account-holding financial institution is considered a “service provider” and any account-holding financial institution has more limited error resolution responsibilities; however that provision does not apply when there is an agreement between the non-account-holding financial institution (the non-bank P2P payment provider) and the account-holding financial institution (the consumer’s depository institution). 12 CFR 1005.14(a). An ACH agreement combined with another agreement to process payment transfers – such as an ACH agreement under which members specifically agree to honor each other’s debit cards – is an “agreement,” and thus this section does not apply. Comment 14(a)-2. Thus, where, as here, an EFT is initiated through a non-bank P2P payment provider using a consumer’s debit card

information, the P2P provider and the account-holding financial institution are parties to an agreement to honor each other's debit cards – the debit card network rules – and the service provider provision in 12 CFR 1005.14, discussed in [Electronic Fund Transfers Coverage: Financial Institutions Question 1](#), does not apply. Accordingly the account-holding financial institution has full error resolution responsibilities.

## Error Resolution

### QUESTION 1:

What is an error for purposes of EFTA and Regulation E?

### ANSWER (UPDATED 12/13/2021):

An error under EFTA and Regulation E includes any of the following:

- An unauthorized EFT.
- An incorrect EFT to or from the consumer's account.
- The omission from a periodic statement of an EFT to or from the consumer's account that should have been included.
- A computational or bookkeeping error made by the financial institution relating to an EFT.
- The consumer's receipt of an incorrect amount of money from an electronic terminal.
- An EFT not identified in accordance with the requirements of 12 CFR 1005.9 or 1005.10(a).
- A consumer's request for any documentation required by 12 CFR 1005.9 or 1005.10(a) or for additional information or clarification concerning an EFT (12 CFR 1005.11(a)(1)).

The term "error" does not include:

- A routine inquiry about the consumer's account balance;
- A request for information for tax or other recordkeeping purposes; or

- A request for duplicate copies of documentation.

Comment 11(a)-6.

**QUESTION 2:**

What are a financial institution's error resolution obligations under Regulation E?

**ANSWER** (UPDATED 12/13/2021):

In general, Regulation E requires that after a financial institution receives oral or written notice of an error from a consumer, the financial institution must do all of the following:

- Promptly investigate the oral or written allegation of error.
- Complete its investigation within the time limits specified in Regulation E.
- Report the results of its investigation within three business days after completing its investigation.
- Correct the error within one business day after determining that an error has occurred.

12 CFR 1005.11(c)(1).

The investigation must be reasonable, including a reasonable review of relevant information within the financial institution's own records. [2019-BCFP-0001](#). The Bureau found that a financial institution did not conduct a reasonable investigation when it summarily denied error disputes if consumers had prior transactions with the same merchant, and the financial institution did not consider other relevant information such as the consumer's assertion that the EFT was unauthorized or for an incorrect amount. [2019-BCFP-0001](#). If the error is an unauthorized EFT, certain consumer liability limits apply. 12 CFR 1005.6.

**QUESTION 3:**

If private network rules provide less consumer protection than federal law, can a financial institution rely on private network rules?

**ANSWER** (UPDATED 6/4/2021):

No. Although private network rules and other agreements may provide additional consumer protections beyond Regulation E, less protective rules do not change a financial institution's

Regulation E obligations. See 15 USC 1693l. For example, some network rules require consumers to provide notice of an error within 60 days of the date of the transaction, even though Regulation E, 12 CFR 1005.11(b)(1)(i), allows consumers to provide notice within 60 days after the institution sends the periodic statement showing the unauthorized transaction. Other network rules allow a financial institution to require a consumer to contact the merchant before initiating an error investigation, even though 1005.11(b)(1) triggers error investigation obligations upon notice from the consumer. The Bureau discussed instances where examiners found financial institutions had violated the 60-day notice requirement in the [Summer 2020 edition of Supervisory Highlights](#).

**QUESTION 4:**

Can a financial institution require a consumer to file a police report or other documentation as a condition of initiating an error resolution investigation?

**ANSWER** (UPDATED 6/4/2021):

No. A financial institution must begin its investigation promptly upon receipt of an oral or written notice of error and may not delay initiating or completing an investigation pending receipt of information from the consumer. See Comments 11(b)(1)-2 and 11(c)-2. In the past, Bureau examiners found that one or more financial institutions failed to initiate and complete reasonable error resolution investigations pending the receipt of additional information required by the institution. These examples can be found in the Bureau's [Summer 2020 edition of Supervisory Highlights](#) and [Fall 2014 edition of Supervisory Highlights](#). The Bureau cited similar violations in [2019-BCFP-0001](#).

## **Error Resolution: Unauthorized EFTs**

**QUESTION 1:**

What is an unauthorized EFT?

**ANSWER** (UPDATED 12/13/2021):

An unauthorized EFT is an 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. 12 CFR 1005.2(m). Unauthorized EFTs include transfers initiated by a person who obtained a consumer's access device through fraud or robbery and consumer transfers at an ATM that were induced by force. Comments 2(m)-3 and 4.

The term unauthorized EFT does not include an EFT initiated through any of the following means:

(1) 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 CFR 1005.2(m)(1). This exclusion does not apply to transfers initiated by a person who obtained a consumer's access device through fraud or robbery. Comment 2(m)-3;

(2) With fraudulent intent by the consumer or any person acting in concert with the consumer. 12 CFR 1005.2(m)(2); or

(3) By the financial institution or its employee, 12 CFR 1005.2(m)(3).

**QUESTION 2:**

If a transfer meets the Regulation E definition of unauthorized EFT, how does a financial institution determine the consumer's liability, if any?

**ANSWER** (UPDATED 6/4/2021):

If a consumer has provided timely notice of an error under 12 CFR 1005.11(b)(1) and the financial institution determines that the error was an unauthorized EFT, the liability protections in Regulation E section 1005.6 would apply. Depending on the circumstances regarding the unauthorized EFT and the timing of the reporting, a consumer may or may not have some liability for the unauthorized EFT. See 12 CFR 1005.6(b).

**QUESTION 3:**

Is an EFT from a consumer's account initiated by a fraudster through a non-bank P2P payment provider considered an unauthorized EFT?

**ANSWER** (UPDATED 12/13/2021):

Yes. Because the EFT was initiated by a person other than the consumer without actual authority to initiate the transfer – *i.e.*, the fraudster – and the consumer received no benefit from the transfer, the EFT is an unauthorized EFT. 12 CFR 1005.2(m). This is true even if the consumer does not have a relationship with, or does not recognize, the non-bank P2P payment provider.

**QUESTION 4:**

Does an EFT initiated by a fraudster using stolen credentials meet the Regulation E definition of an unauthorized EFT?

**ANSWER** (UPDATED 12/13/2021):

Yes. As discussed in [Electronic Fund Transfers Error Resolution: Unauthorized EFT Question 1](#), Regulation E defines an unauthorized EFT as a transfer 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. 12 CFR 1005.2(m). When a consumer's account access information is obtained from a third party through fraudulent means such as computer hacking, and a hacker uses that information to make an EFT from the consumer's account, the transfer is an unauthorized EFT under Regulation E.

For example, the Bureau is aware of the following situations involving unauthorized EFTs:

- A consumer shares their account access information in order to enter into a transaction with a third party, such as a merchant, lender, or employer offering direct deposit, and a fraudster obtains the consumer's account access information by hacking into the computer system of the third party. The fraudster then uses a bank-provided P2P payment application to initiate a credit push payment out of the consumer's deposit account.
- A consumer shares their debit card information with a P2P payment provider in order to use a mobile wallet. A fraudster then hacks into the consumer's phone and uses the mobile wallet to initiate a debit card transfer out of the consumer's deposit or prepaid account.
- A thief steals a consumer's physical wallet and initiates a payment using the consumer's stolen debit card.

See [Electronic Fund Transfers Error Resolution: Unauthorized EFTs Question 5](#) for more examples of unauthorized EFTs.

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 discussed in [Electronic Fund Transfers Error Resolution Question 2](#), as well as the liability protections for unauthorized transfers in 12 CFR 1005.6.



**QUESTION 5:**

A third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account. Does the transfer meet Regulation E's definition of an unauthorized EFT?

**ANSWER** (UPDATED 6/4/2021):

Yes. As discussed in Electronic Fund Transfers Error Resolution: Unauthorized Fund Transfers Question 1, Regulation E defines an unauthorized EFT as an 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. 12 CFR 1005.2(m). Comment 1005.2(m)-3 explains further that an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery. Similarly, 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.

For example, the Bureau is aware of the following situations where a third party has fraudulently obtained a consumer's account access information, and thus, are considered unauthorized EFTs under Regulation E: (1) a third-party calling the consumer and pretending to be a representative from the consumer's financial institution and then tricking the consumer into providing their account login information, texted account confirmation code, debit card number, or other information that could be used to initiate an EFT out of the consumer's account, and (2) a third party using phishing or other methods to gain access to a consumer's computer and observe the consumer entering account login information. EFTs stemming from these situations meet the Regulation E definition of unauthorized EFTs.

**QUESTION 6:**

If a third-party fraudulently induces a consumer to share account access information, are subsequent transfers initiated with the fraudulently obtained account information excluded from Regulation E's definition of unauthorized electronic fund transfer because they are initiated "[b]y a

person who was furnished the access device to the consumer's account by the consumer”?

**ANSWER** (UPDATED 6/4/2021):

No. A consumer who is fraudulently induced into providing account information has not furnished an access device under Regulation E. As explained above in [Electronic Fund Transfers Error Resolution: Unauthorized EFTs 3, 4, and 5](#), EFTs initiated using account access information obtained through fraud or robbery fall within the Regulation E definition of unauthorized EFT. See Comment 1005.2(m)-3.

**QUESTION 7:**

Can a financial institution consider a consumer's negligence when determining liability for unauthorized EFTs under Regulation E?

**ANSWER** (UPDATED 6/4/2021):

No. Regulation E sets forth the conditions in which consumers may be held liable for unauthorized transfers, and its commentary expressly states that negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E. 12 CFR 1005.6; Comment 6(b)-2. For example, consumer behavior that may constitute negligence under state law, such as situations where the consumer wrote the PIN on a debit card or on a piece of paper kept with the card, does not affect the consumer's liability for unauthorized transfers under Regulation E. Comment 1005.6(b)-2.

**QUESTION 8:**

If a financial institution's agreement with a consumer includes a provision that modifies or waives certain protections granted by Regulation E, such as waiving Regulation E liability protections if a consumer has shared account information with a third party, can the institution rely on its agreement when determining whether the EFT was unauthorized and whether related liability protections apply?

**ANSWER** (UPDATED 6/4/2021):

No. EFTA includes an anti-waiver provision stating that “[n]o writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or cause of action created by [EFTA].” 15 U.S.C. § 1693l. Although there may be circumstances where a consumer has provided actual authority to a third

party under Regulation E according to 12 CFR 1005.2(m), an agreement cannot restrict a consumer's rights beyond what is provided in the law, and any contract or agreement attempting to do so is a violation of EFTA.

**QUESTION 9:**

If a consumer provides notice to a financial institution about an unauthorized EFT, can the financial institution require that the consumer first contact the merchant about the potential unauthorized EFT before the financial institution initiates its error resolution investigation?

**ANSWER** (UPDATED 6/4/2021):

No. A financial institution must begin its investigation promptly upon receipt of an oral or written notice of error and may not delay initiating or completing an investigation pending receipt of information from the consumer. See Comments 11(b)(1)-2 and 11(c)-2. For example, in [2019-BCFP-0001](#), the Bureau found that the practice of requiring a consumer to contact the merchant before initiating an error resolution investigation was a violation of Regulation E. Similarly, the [Fall 2014 edition of Supervisory Highlights](#) discussed instances where examiners found that one or more financial institutions had instructed consumers to contact the merchant instead of promptly initiating an error investigation.

**QUESTION 10:**

Do private network rules, such as provisions that a transfer is final and irrevocable, impact whether a P2P credit-push transfer meets the Regulation E definition of unauthorized EFT?

**ANSWER** (UPDATED 12/13/2021):

No. Although private network rules and other commercial agreements may provide for interbank finality and irrevocability, they do not reduce consumer protections against liability for unauthorized EFTs afforded by the Electronic Fund Transfer Act. See 15 USC 1693g(e). Moreover, no agreement between a consumer and any other person may waive any right provided by the EFTA. See 15 USC 1693i. Accordingly, any financial institution in this transaction must comply with the error resolution requirements discussed in [Electronic Fund Transfers Error Resolution Question 2](#), as well as the liability protections for unauthorized transfers.

**QUESTION 11:**

A fraudster initiates an EFT through a non-bank P2P payment provider that the consumer does not have a relationship with from the consumer's account with a depository institution. Is the depository institution considered a financial institution with full error resolution obligations under Regulation E?

**ANSWER** (UPDATED 12/13/2021):

Yes. As discussed in [Electronic Fund Transfers Coverage: Financial Institutions Question 1](#), the definition of financial institution includes a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide EFT services. 12 CFR 1005.2(i). Here, the account-holding financial institution holds the consumer's account, and is thus considered a financial institution under Regulation E. Any entity defined as a financial institution under Regulation E has error resolution obligations in the event that a consumer notifies the financial institution of an error, with limited exceptions. 12 CFR 1005.11. As discussed in [Electronic Fund Transfers Error Resolution: Unauthorized Transfers Question 4](#), since the transaction is an unauthorized EFT, the depository institution must comply with any applicable liability protections for unauthorized transfers in 12 CFR 1005.6.