HUNTON
ANDREWS KURTH

Regulation E and the Electronic Funds Transfer Act

All Clear or Clear As Mud?

Aliza Pescovitz Malouf
Associate – Financial Services Litigation and Compliance
Hunton Andrews Kurth LLP
amalouf@huntonak.com
214-979-8229
July 21, 2022

Issues for Discussion

REGULATION E

ELECTRONIC FUND TRANSFER ACT

Purpose of Reg E/EFTA

"[E]stablish the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer and remittance transfer services and of financial institutions or other persons that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers and remittance transfers."

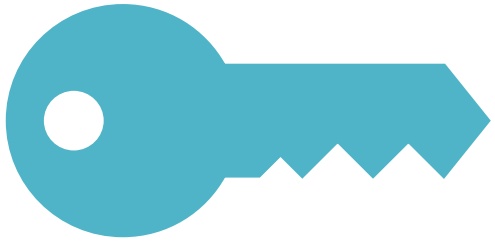
Why does EFTA/Reg E Matter?

Peer-to-Peer Transfer Applications – used to transfer money electronically – e.g. Venmo or Zelle.

In 2017, only 57% of American adults used a P2P app. In 2020, the number increased to 70%.

PayPal, Venmo, Zelle, Google Pay and Square Cash all roughly doubled in use since 2017.

Between 2017 and June 2021, the CFPB received roughly 9,277 consumer complaints related to mobile or digital wallets. More than 5,200 were filed between April 2020 and May 2021.



KEY DEFINITIONS

SURVEY Question 1

Is your company a "Financial Institution" for under Regulation E?

A. Yes

B. No

C. Unsure

Financial Institution

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

- Any 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 EFT services.

What is an EFT ?

- Automated Teller Machines (ATM)
- Point of Sale Transactions
- Automated Clearing House (ACH)
- Direct Deposits or Withdrawals
- Debit Card Transactions
- P2P Payment

Access Device

Card, code or other means of access to a consumer's account that may be used by the consumer to initiate EFTs

Becoming an Accepted Access Device

- Requests (via written request or oral request)
- Uses the device to transfer money between accounts or to obtain money, property, or services
- Requests the validation of an access device issued without solicitation
- Receives a renewal of, or substitute for, an existing access device from either the financial institution that issued the original access device or that institution's successor.

Unauthorized Electronic Funds Transfers

"Unauthorized electronic fund transfer" means an electronic fund 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."

Unauthorized EFTs Include

- Transfers initiated as a result of theft of an access device
- EFTS at an ATM if the consumer is induced by force to initiate the EFT Transfers initiated as a result of fraud
- Transfers initiated as a result of fraud

Common Examples of Unauthorized EFTs

- Third Party Computer Hack
- Hack of Consumer's Phone
- Physical Theft
- Fraudster Pretending to be a Consumer's Financial Institution
- Phishing

Liability for Unauthorized Transfers

General Rule . . .

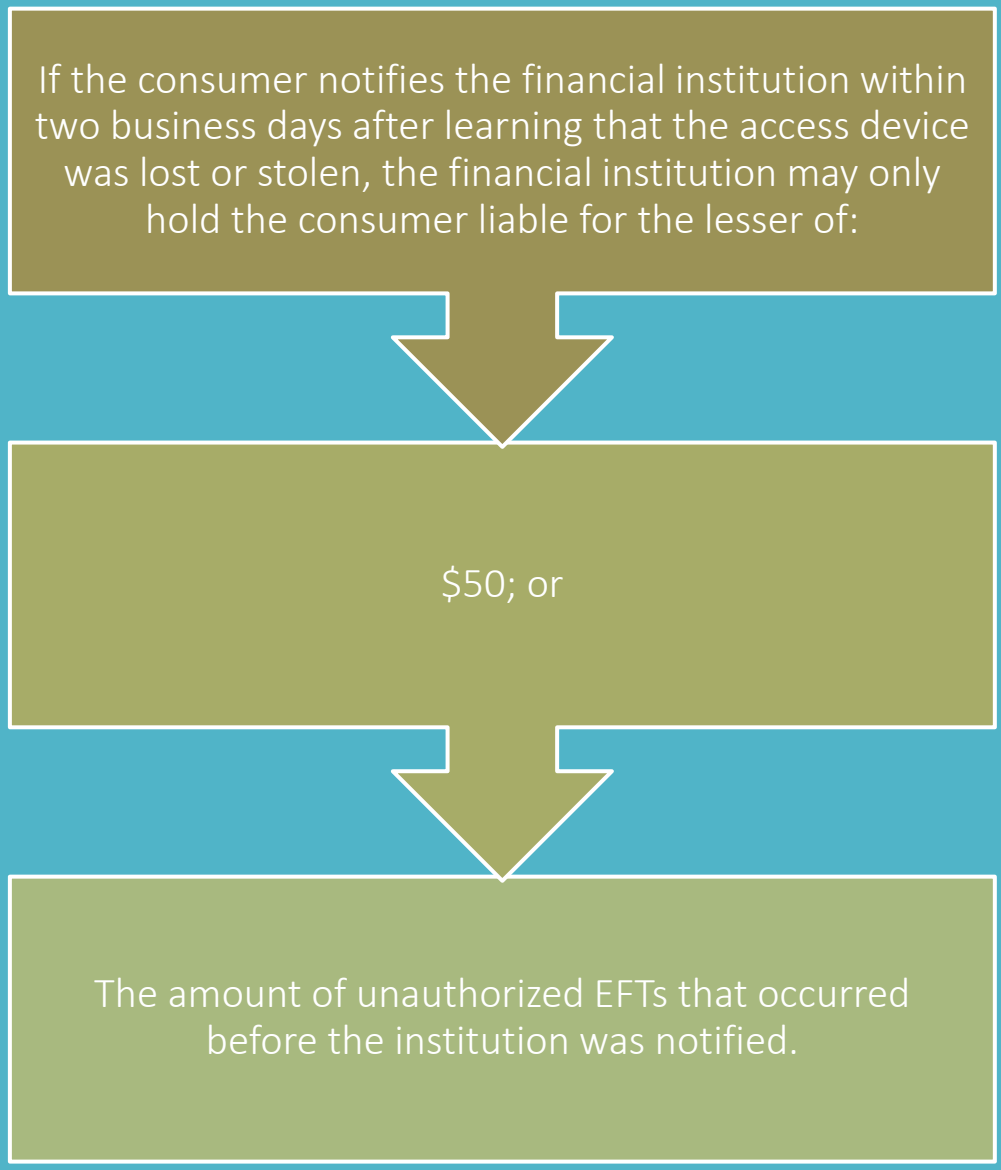
The financial institution is responsible for unauthorized electronic funds transfers

Disclosures Required to Shift Liability

- Amount of Liability
- Contact Information for Notice
- Business Days

Consumer Liability for Unauthorized EFTS

First-Tier Liability



Second-Tier Liability

If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of $500 or the sum of:

- $50 or the amount of unauthorized transfers that occur within the two business days, whichever is less; and
- The amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period.

Third-Tier Liability

A consumer must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. If the consumer fails to do so, the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not have occurred had the consumer notified the institution within the 60-day period.

Survey Question 2

How many notices of error does your financial institution receive on a weekly basis?

A. None. We don't receive notices of error.
B. Less than 1
C. 1-15
D. 15-50
E. Over 50

Error Resolution Procedures

Unauthorized EFTS Are Errors Under Reg E?

- The CFPB has recently clarified that the following scenarios constitute unauthorized electronic funds:
  - *An EFT from a consumer's account initiated by a fraudster through a non-bank P2P payment provider*
  - *An EFT initiated by a fraudster using stolen credentials*
  - *An EFT initiated by a fraudster after fraudulently inducing a consumer into sharing account access information.*

Notice of Error Requirements

- Must be received by the financial institution no later than 60 days after the institution sends the period statement first showing the error
- Enables the financial institution to identify the consumer's name and account number
- Indicates why the consumer believes an error exists and includes to the extent possible the type, date and amount of the error

Error Resolution Procedures

After a financial institution receives oral or written notice of an error from a consumer, the financial institution must do all 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.*

Provisional Credit

Must be in the amount of the alleged error

Must be provided within 10 business days of receiving the notice of error

Provide notice to the consumer of the provisional credit within 2 days of providing the credit

Give the consumer full use of the funds during the investigation

Correct any errors within 1 business day

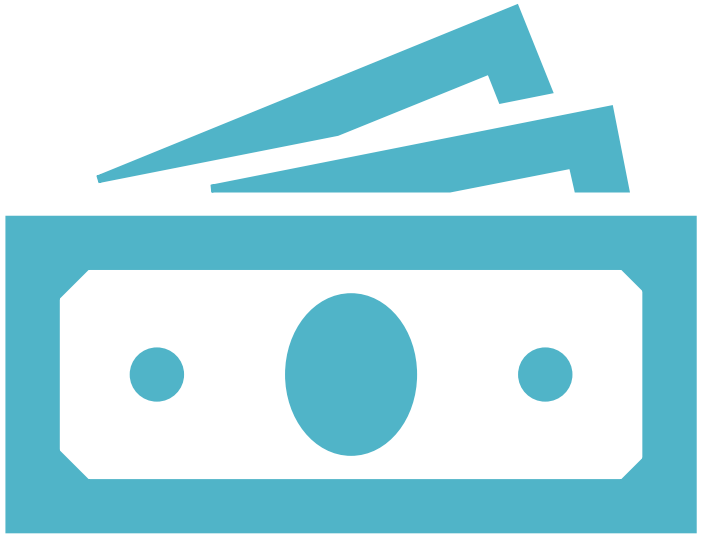
Report results to consumer within 3 business days

Results of an Investigation

No Error Finding

Different Error Finding

Finding of Error



Damages

Civil Liability for Individual Actions

- Any actual damages
- Statutory Damages
- Attorney's fees and costs
- Treble Damages

Consent Orders & Enforcement Actions

The CFPB can also seek civil money penalties and consent orders have ranged into the millions of dollars.

AGENCY GUIDANCE

CFPB FAQs - June 4, 2021

- Unauthorized transfers include situations where a consumer is fraudulently induced by a third party into sharing account access information.
- Negligence by the consumer cannot be used to increase the liability limits that may be imposed on consumers.
- Financial Institutions may not rely on private network rules to limit liability.
- Financial Institutions must begin investigation promptly upon receipt of notice of error.
- Financial Institutions may not require a consumer to dispute a transfer with the merchant before initiating an error investigation.
- Financial Institutions may not require a consumer to file a police report as a condition of initiating an error resolution investigation.

CFPB FAQs – December 13, 2021

- Any P2P payment that meets the definition of an EFT is covered by the EFTA/Reg E.
- The term “financial institution” includes P2P providers and is subject to error resolution procedures.
- A dispute investigation must be reasonable.
- CFPB reiterated its guidance from the June 4 FAQs that (1) transfers initiated as a result of fraud are not authorized; (2) a financial institution may not require a dispute with the merchant or a police report prior to investigating; and (3) a financial institution cannot implement policies and procedures that are less protective than the EFTA.

Most Common Errors Identified by CFPB – Summer 2021

Most common EFTA/Regulation E violations identified by the CFPB include:

- Requiring written confirmation of an oral notice of error before investigating;
- Requiring consumers to contact merchants about alleged unauthorized transactions before investigating;
- Relying on incorrect dates to assess the timeliness of an EFT error notice;
- Failing to provide an explanation or an accurate explanation of investigation results when determining no error or a different error occurred; and
- Failing to include in the error investigation report a statement regarding a consumer's right to obtain the documentation that an institution relied on in its error investigation.

Most Common Errors Identified by CFPB – Fall 2021

Most common EFTA/Regulation E violations identified by the CFPB in the Fall of 2021 include:

- Financial institutions included language in Terms of Use waiving a consumer's rights to make a stop payment request for preauthorized transfers and failed to honor stop payment requests;
- Failure to provide a written explanation of a "no error" or "different error" finding – CFPB also clarified that "an 'explanation' is not synonymous with that of a 'determination.' Financial institutions must go beyond just providing their findings and actually explain those findings";
- Failure to comply with timing requirements for investigation, completion, and reporting of results in response to a dispute.

FDIC Supervisory Highlights – March 2022

Consumer account disclosures cannot limit protections under Reg E.

Financial institution, as account holding institution, is responsible under Reg E for fraudulent EFTs conducted through money payment platforms ("MPPs") such as Cash App, Zelle, or Venmo. The MPP is also responsible under Reg E as a "financial institution."

Reg E also applies to P2P transfers made through MPPs, and both the MPP and financial institution are obligated to investigate the EFT dispute.

FDIC Identified Steps to Improve Regulation E Compliance

- Reviewing account agreements and disclosures
- Conduct thorough investigation
- Provide documents upon request
- Educating consumers
- Encourage consumers to provide notice
- Implement fraud detection and prevention measures
- Improve training

Best Practices

Survey Question 3

Has your financial institution instituted any preventative measures in order to avoid risk from unauthorized funds transfers?

A. Yes. They're great.

B. Yes. But they could use some work.

C. No.

D. Unsure

Best Practices

- Impose account-level limitations to reduce the risk of loss;
- Limit the frequency of P2P transactions;
- Set-up consumer alerts with holds to mitigate against the risk of loss, or even block certain P2P applications with higher levels of incidents of fraud entirely;
- Implement policies and procedures to actively monitor accounts and freeze transactions before they go through to prevent fraud on the front end.

QUESTIONS

Aliza Malouf
214-979-8229
amalouf@huntonAK.com