NAFCU Credit Union Compliance

GPS MANUAL

National Association of Federally-Insured Credit Unions

Official textbook for our award-winning NAFCU Certified Compliance Officer Program
# Chapter 2 – Member Accounts

## Section 2

### Regulation E

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>107</td>
</tr>
<tr>
<td>Which Accounts Are Covered</td>
<td>107</td>
</tr>
<tr>
<td>Which Transactions Are Covered</td>
<td>107</td>
</tr>
<tr>
<td>Account Opening Disclosures</td>
<td>108</td>
</tr>
<tr>
<td>Periodic Statement Requirement</td>
<td>108</td>
</tr>
<tr>
<td>Error Resolution Notice</td>
<td>109</td>
</tr>
<tr>
<td>Change-in-Terms Notices</td>
<td>109</td>
</tr>
<tr>
<td>Disclosures at Automated Teller Machines (ATMs)</td>
<td>109</td>
</tr>
<tr>
<td>Unauthorized Transfers and Member Liability</td>
<td>110</td>
</tr>
<tr>
<td>Special Situations</td>
<td>110</td>
</tr>
<tr>
<td>Member Notification of Unauthorized Transactions</td>
<td>111</td>
</tr>
<tr>
<td>Timely Notice of Loss or Theft Given</td>
<td>111</td>
</tr>
<tr>
<td>Timely Notice of Loss or Theft Not Given</td>
<td>112</td>
</tr>
<tr>
<td>Timely Notice Not Given After Periodic Statement Delivered</td>
<td>113</td>
</tr>
<tr>
<td>Error Resolution Process</td>
<td>114</td>
</tr>
<tr>
<td>Time Limits for Error Review</td>
<td>114</td>
</tr>
<tr>
<td>Investigation Pending Receipt of Information</td>
<td>116</td>
</tr>
<tr>
<td>Notification of Investigations</td>
<td>116</td>
</tr>
<tr>
<td>Prohibition on Requiring Electronic Payment of Loans</td>
<td>117</td>
</tr>
<tr>
<td>Overdraft Rules for ATM and One-Time Debit Card Transactions</td>
<td>117</td>
</tr>
<tr>
<td>Opt-In Process</td>
<td>118</td>
</tr>
<tr>
<td>Prohibition on Conditioning and Same Terms Requirement</td>
<td>118</td>
</tr>
<tr>
<td>Duration of Opt-in and Right to Revoke</td>
<td>119</td>
</tr>
<tr>
<td>Remittance Transfers</td>
<td>120</td>
</tr>
<tr>
<td>What is a Remittance Transfer?</td>
<td>120</td>
</tr>
<tr>
<td>Definitions</td>
<td>120</td>
</tr>
<tr>
<td>Safe Harbor</td>
<td>122</td>
</tr>
<tr>
<td>Disclosure Requirements</td>
<td>123</td>
</tr>
<tr>
<td>Pre-Payment Disclosures</td>
<td>123</td>
</tr>
<tr>
<td>Receipts</td>
<td>124</td>
</tr>
<tr>
<td>Combined Disclosures</td>
<td>125</td>
</tr>
</tbody>
</table>
Format, Delivery and Timing ................................................................. 125
Error Resolution .................................................................................. 126
Cancellation ......................................................................................... 127
Resources and Research Tips............................................................ 127
Overview

Regulation E implements the Electronic Funds Transfer Act (EFTA) and covers numerous issues related to electronic transactions. This section will describe the types of accounts and transactions that are subject to Regulation E as well as the credit union’s requirements under Regulation E.

Which Accounts Are Covered

It is important to understand the coverage of Regulation E because the protections do not extend to all types of accounts. The definition of “account” includes consumer asset accounts such as savings, checking and payroll cards held directly or indirectly by the credit union and established primarily for personal, family or household purposes. This definition does not extend to business purpose accounts, accounts held under a trust agreement or escrow accounts.

Which Transactions Are Covered

Regulation E defines “electronic funds transfer” as “any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account.” Section 1005.3(b) gives examples of transactions included in this definition:

- Point–of–sale (POS) transfers – including both PIN–based and signature–based;
- ACH transfers;
- ATM transfers;
- Direct deposit or withdrawal of funds;
- Transfers initiated by telephone;
- Transfers initiated by debit card transactions – regardless of whether conducted through an electronic terminal;
- Electronic transfers initiated using information from a paper check; and
- Online bill payments.
The regulation also indicates areas that do not fall under Regulation E's control, including paper checks, wire transfers¹ and certain automatic transfers occurring within the same financial institution.

Whether or not a transaction is covered by Regulation E will depend on the facts and circumstances of each case and credit unions should review the definition and staff commentary when making determinations rather than relying solely on a preprinted list of transactions. Remember, the regulations are not updated as often as new types of transfers are created and adopted by financial institutions. For example, text message transfers are not listed in Regulation E, but still could be covered under the regulation depending on how the transfer is processed.

### Account Opening Disclosures

Regulation E requires the credit union to provide disclosures at account opening and throughout the relationship. At account opening, the disclosures must be provided at the time the service is established or before the first electronic funds transfer is made. The account opening disclosure must provide the member with information about the types of transactions the member may make, any fees associated with those transactions and potential liability for unauthorized transactions. Additional information about the content of account opening disclosures can be found in section 1005.7(b). The account opening disclosures can be included with other disclosures, such as Truth in Savings disclosures, and can be provided electronically subject to E-SIGN requirements.

### Periodic Statement Requirement

Section 1005.9(b) contains a periodic statement requirement for accounts to or from which an electronic funds transfer can be made. The timing depends on whether or not an electronic funds transfer has been conducted in the preceding months and not whether the account has the ability to conduct an electronic funds transfer.

If no electronic funds transfers have occurred, the credit union is only required to send periodic statements on a quarterly basis. However, if an electronic funds transfer has occurred in the prior month, the rule requires the credit union to send a statement for that month. The staff commentary indicates that if the credit union usually sends statements quarterly it must send interim statements corresponding to the month where an electronic

---

¹ Under the CFPB’s rules on remittance transfers, Subpart B to Regulation E covers international consumer wire transfers. Historically, wire transfers have been governed by state law through enactment of Article 4A of the Uniform Commercial Code. Commercial wire transfers are not affected by this change.
funds transfer has occurred. Thus, if the credit union usually sends periodic statements at
the end of March, June, September and December, and the member conducts electronic
funds transfers in February and October, the credit union would need to send a periodic
statement for those months in addition to its regular quarterly statements.

Error Resolution Notice

As part of its disclosure requirements, Regulation E requires credit unions to send both an
initial and annual error resolution notice to members who have accounts subject to
Regulation E (i.e., the member has the ability to make electronic funds transfers). This
notice informs members how to report errors or ask questions regarding electronic
transfers. Under section 1005.7(b), the initial notice must be provided “at the time a
consumer contracts for an electronic fund transfer service or before the first electronic fund
transfer is made involving the consumer’s account.” Practically speaking, this generally
means at account opening. Under section 1005.8(b), the annual notice can be sent once a
year or, alternatively, can be included as an abbreviated notice on each periodic statement.
Both approaches meet the annual notice requirement and Appendix A to Regulation E
includes model forms for both initial and annual notices (Model Form A-3).

Change-in-Terms Notices

Similar to other regulations, credit unions have a requirement to provide advance
notification to members when certain terms of the account are changed. For Regulation E,
the notice must be given at least 21 days prior to the effective date of the change. There is
no specific wording or format required for the change-in-terms notice nor is there a model
form. The notice can be included on or with a periodic statement or sent as a separate
mailing.

A change-in-terms notice must be sent if the credit union: increases fees; increases potential
liability for members; removes types of funds transfer options under the account; or
increases the limitations on the frequency or dollar amount of transfers. A notice is not
required if the credit union closes ATMs or cancels a member’s debit card.

Disclosures at Automated Teller Machines (ATMs)

On December 20, 2012, the Electronic Funds Transfer Act (EFTA) was amended. This
amendment removed a federal requirement to place a physical notice on the ATM itself
that a fee will be charged for an electronic funds transfer. However, credit unions are still
required to provide the notice on the ATM screen or via a printed piece of paper prior to the consumer completing a transaction where a fee will be charged. Section 1005.16 of Regulation E contains the ATM notice requirements. Although neither the EFTA nor Regulation E requires the physical notice, there is no reason to remove the existing notices from the machines. The extra notice provided by the sign is still a service to member and non-member ATM users.

Note this amendment to the EFTA removed the federal requirement to post physical notices on ATMs. There may be state law requirements that still require a physical notice on ATMs. Therefore, credit unions might want to check with local counsel regarding any state law that might impact the credit union.

Unauthorized Transfers and Member Liability

Regulation E provides limitations on the amount of member liability for unauthorized transactions. The member’s potential liability depends on when the member provides notification of the unauthorized transactions. Additionally, any agreements with network providers – such as VISA or MasterCard – could further limit member liability by agreeing to fully reimburse the member for any unauthorized transactions.

Initially, it is important to understand the definition of “unauthorized electronic funds transfer,” which is an “electronic funds 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.”

Special Situations

The regulation states the definition of unauthorized electronic funds transfer does not include a situation where the member acts with fraudulent intent or a transaction conducted in concert with the member. For example, if a member gives his brother his ATM card and PIN with the understanding the brother will withdraw money and the member will claim an unauthorized transfer – this transaction might not fall under the definition of an “unauthorized electronic funds transfer.”

If the member provides another person with authorization to make transfers from the account, the member can be held fully liable if the other person exceeds their authority or continues to make transfers after the authority has been removed – provided the member has not notified the credit union of the revocation of authority. This makes sense as the member has provided the authorization to the other person that prevents the transfers from being unauthorized. If the member revokes the authority in June and notifies the credit
union of the revocation, further transfers by the other person in July and August could be considered unauthorized funds transfers.

If the member’s account is accessed as a result of a robbery or fraud, such as phishing or card skimming, the transactions are unauthorized. Similarly, if a member is forced to conduct a transaction (i.e., forced to input their card and PIN at an ATM under threat of violence), the transactions are unauthorized even though the member was the one who conducted the transaction.

In situations where the member has been negligent with their debit card or account information, the credit union cannot push higher liability onto the member. The credit union is still required to follow the liability thresholds laid out in section 1005.6. Here is the language from the staff commentary:

“Negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E. Thus, consumer behavior that may constitute negligence under state law, such as writing 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.”

Similarly, the staff commentary indicates the credit union cannot have members agree to accept greater potential liability for unauthorized transactions under Regulation E. Think of the liability thresholds as maximums – if the member provides the required notice within the required timeframe the credit union cannot hold the member liable for more than the amount in Regulation E.

**Member Notification of Unauthorized Transactions**

The amount of liability that can be passed on to the member for unauthorized transactions depends on the timing of the member’s notification to the credit union. Importantly, notification is deemed to be given whenever the relevant information is given to the credit union regardless of whether the information is properly relayed to the fraud department. Notification can be made in person, by telephone or in writing.

**Timely Notice of Loss or Theft Given**

There are two separate liability levels that apply, which depend on the timing of the member’s notification about the loss or theft of an access device. ”Access device” is defined in section 1005.2(a)(1) as “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 funds transfers.” If the member provides notification within two business days of learning
of the loss or theft, the member’s liability cannot exceed $50. The staff commentary includes an example that makes clear the timeframe depends on when the member “learns of the loss” not when the actual loss occurs:

“The basic liability limit is $50. For example, the consumer’s card is lost or stolen on Monday and the consumer learns of the loss or theft on Wednesday. If the consumer notifies the financial institution within two business days of learning of the loss or theft (by Friday at midnight), the consumer’s liability is limited to $50 or the amount of the unauthorized transfers that occurred before notification, whichever is less.”

**Timely Notice of Loss or Theft Not Given**

If the member does not notify the credit union within two business days of learning of the loss or theft, the member’s liability can reach up to $500 for the unauthorized transactions. However, the amount of the member’s liability is not a straightforward $500 amount. Rather, the credit union needs to follow the guidelines in Regulation E to determine the member’s liability – which will depend on when the unauthorized transactions took place. The guidelines give a two-part test that allows the credit union to hold the member liable for up to $50 of the unauthorized transactions that occurred within two business days after the member learned of the loss. The second part also allows the credit union to hold the member liable for $450 (making it $500 total) for transactions that took place after the two business day period ended and before notification to the credit union – provided the credit union can determine it would have been able to prevent the transactions (such as by freezing the debit card). If no transactions were conducted in the first two business days after the member learned of the loss, the member could be held liable for up to $500 on transactions conducted after the end of the two business days and before notification.

The staff commentary to section 1005.6(b)(2) provides an example of how these two tiers of liability work together that may be useful:

“The consumer's card is stolen on Monday and the consumer learns of the theft that same day. The consumer reports the theft on Friday. The $500 limit applies because the consumer failed to notify the financial institution within two business days of learning of the theft (which would have been by midnight Wednesday). How much the consumer is actually liable for, however, depends on when the unauthorized transfers take place. In this example, assume a $100 unauthorized transfer was made on Tuesday and a $600 unauthorized transfer on Thursday. Because the consumer is liable for the amount of the loss that occurs within the first two business days (but no more than $50), plus the amount of the unauthorized transfers that occurs after the first two business days and before the consumer gives notice, the consumer's total liability is $500 ($50 of the $100 transfer plus $450 of the $600
transfer, in this example). But if $600 was taken on Tuesday and $100 on Thursday, the consumer's maximum liability would be $150 ($50 of the $600 plus $100).”

As you can see, determining what liability tier applies, and how much the member is liable for, will depend on when the member “learned of the loss.”

Both of these provisions use the timing of when the member “learned of the loss” rather than when the transactions occurred. Thus, in practice, the higher liability level is only applicable in situations where the member has learned of the loss and fails to follow up with the credit union and provide notification within two business days.

There is some difficulty built-in to these member liability provisions. Credit unions may find it challenging to know when the member “learned of the loss” or to prove the member knew of the loss at a prior time. These are difficult issues and Regulation E does not provide definitive guidance. The staff commentary does state that the fact a member has received a periodic statement with unauthorized transactions can be used as a factor in determining if the member knew of the loss of an access device but it cannot be considered conclusive evidence. In the end, the determination of when a member “learned of the loss” may ultimately be decided by a court.

**Timely Notice Not Given After Periodic Statement Delivered**

Regulation E does include another liability threshold based on when a periodic statement containing the unauthorized transaction is sent to the member. This threshold works in combination with the other two tiers of member liability, discussed earlier, and does not supersede those requirements. In other words, if the member is severely late in notifying the credit union it does not mean the member's liability is unlimited as the prior maximum liability levels remain in place.

Section 1005.6(b)(3) indicates the member can be held fully liable for unauthorized transactions that occur more than sixty days after the delivery of a periodic statement and prior to notice to the credit union. The member's liability may still be limited to a maximum of $50 or $500 for transactions within sixty days after the periodic statement showing the first unauthorized transactions was delivered.

The first two tiers of liability only apply to unauthorized transfers from a member’s account made with an access device. If no access device was used to make an unauthorized transfer, section 1005.6(b)(3) is the only liability threshold that applies. For more details on the intricacies of the member liability sections of Regulation E, see the staff commentary to section 1005.6, which contains additional information and examples.