NAFCU Credit Union Compliance

ROADMAP

Your Companion for Navigating Federal Credit Union Regulations

NAFCU
National Association of Federally-Insured Credit Unions

Official textbook for our award-winning NAFCU Certified Compliance 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>102</td>
</tr>
<tr>
<td>Scope</td>
<td>102</td>
</tr>
<tr>
<td>Covered Accounts</td>
<td>102</td>
</tr>
<tr>
<td>Covered Transactions</td>
<td>102</td>
</tr>
<tr>
<td>Account Opening Disclosures</td>
<td>103</td>
</tr>
<tr>
<td>Subsequent Disclosures</td>
<td>104</td>
</tr>
<tr>
<td>Periodic Statement Disclosures</td>
<td>104</td>
</tr>
<tr>
<td>Error Resolution Notice</td>
<td>104</td>
</tr>
<tr>
<td>Change-in-Terms Notices</td>
<td>105</td>
</tr>
<tr>
<td>Unauthorized Transfers</td>
<td>105</td>
</tr>
<tr>
<td>Error Resolution Procedures</td>
<td>106</td>
</tr>
<tr>
<td>Investigation Requirements</td>
<td>106</td>
</tr>
<tr>
<td>Member Liability</td>
<td>108</td>
</tr>
<tr>
<td>Loss or Theft of an Access Device</td>
<td>108</td>
</tr>
<tr>
<td>No Access Device Used</td>
<td>109</td>
</tr>
<tr>
<td>Prohibition on Requiring Electronic Payment of Loans</td>
<td>110</td>
</tr>
<tr>
<td>Overdraft Rules for ATM and One-Time Debit Card Transactions</td>
<td>110</td>
</tr>
<tr>
<td>Opt-In Process</td>
<td>111</td>
</tr>
<tr>
<td>Duration of Opt-in and Right to Revoke</td>
<td>111</td>
</tr>
<tr>
<td>Prohibition on Conditioning and Same Terms Requirement</td>
<td>112</td>
</tr>
<tr>
<td>Prepaid Accounts</td>
<td>112</td>
</tr>
<tr>
<td>Disclosures</td>
<td>114</td>
</tr>
<tr>
<td>Pre-Acquisition Disclosures</td>
<td>114</td>
</tr>
<tr>
<td>Periodic Statement Disclosures</td>
<td>114</td>
</tr>
<tr>
<td>Error Resolution Procedures and Liability</td>
<td>115</td>
</tr>
<tr>
<td>Remittance Transfers</td>
<td>116</td>
</tr>
<tr>
<td>Disclosures</td>
<td>116</td>
</tr>
<tr>
<td>Cancellation</td>
<td>117</td>
</tr>
<tr>
<td>Error Resolution Procedures</td>
<td>117</td>
</tr>
</tbody>
</table>
OVERVIEW

Regulation E (12 CFR Part 1005) implements the Electronic Funds Transfer Act (EFTA). It covers the disclosure requirements, liability limits and other member protections related to electronic fund transfers and remittance transfers. These requirements will be reviewed throughout this section.

SCOPE

It is important to understand the coverage of Regulation E because the requirements and protections do not extend to all types of accounts or all types of electronic transfers. In general, Regulation E applies to electronic fund transfers that are debited or credited to a member’s account by a credit union.

Covered Accounts

Section 1005.2(b)(1) defines “account” to include member 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.

Covered Transactions

An “electronic fund transfer” (EFT) is defined in section 1005.3(b) 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)(1) and its commentary give 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; and
- Online bill payments.
The regulation also gives examples of transactions that are not electronic fund transfers: paper checks, wire transfers and certain automatic transfers occurring within the same credit union.

Whether or not a transaction is considered an electronic fund transfer 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.

**RESEARCH TIP:** The CFPB’s examination manual on the EFTA can be a useful tool in researching Regulation E issues as it provides some additional details about the regulation’s coverage and requirements.

### ACCOUNT OPENING DISCLOSURES

Section 1005.7 requires credit unions to provide certain information about the account at the time the account is opened. This information includes:

- **Liability information.** A summary of the member’s liability for unauthorized EFTs and the telephone number and address to notify the credit union of unauthorized EFTs;
- **Error resolution information.** A notice describing the credit union’s error resolution responsibilities;
- **Business days.** The credit union’s business days;
- **EFT limitations.** Types of EFTs the member may make and any limitations on the frequency or dollar amount;
- **Fees.** Fees imposed for EFTs;
- **Documents.** A summary of the member’s right to receipts, periodic statements and preauthorized transfer notices; and
- **Stop payment.** A summary of the member’s right to and procedures for stopping payment of a preauthorized EFT.

These disclosures must be provided at the time the EFT service is established or before the first EFT is made. The account opening disclosures can be included with other disclosures, such as Truth in Savings disclosures, and can be provided electronically subject to the E-SIGN Act’s requirements.
SUBSEQUENT DISCLOSURES

In addition to the disclosures required when an account is opened, Regulation E also requires disclosures throughout the account relationship.

**Periodic Statement Disclosures**

Section 1005.9(b) requires a periodic statement for accounts to or from which an EFT can be made. The following information must be included on each periodic statement:

- EFT transaction information such as the amount, date and payee;
- Account number;
- Fees imposed;
- Account balances at the start and end of the statement period;
- Telephone number and address to report unauthorized EFTs; and
- Telephone number to confirm preauthorized transfers.

The timing for periodic statements depends on whether or not an EFT has been conducted in the preceding months. If no EFTs have occurred, the credit union is only required to send periodic statements on a quarterly basis. However, if an EFT 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 funds transfer has occurred.

**EXAMPLE**

If a credit union usually sends quarterly periodic statements at the end of March, June, September and December, and the member conducts EFTs 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 that informs members how to report errors or ask questions regarding EFTs. Under section 1005.7(b), the initial notice must be provided with the account opening disclosures. 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. 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, section 1005.8(a) requires notice to members when certain terms of the account are changed. 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.

**UNAUTHORIZED TRANSFERS**

Regulation E requires credit unions to investigate claims related to unauthorized EFTs and limits the amount of liability credit unions can pass on to members for these transfers. To understand when these rules apply it is important to start with the definition of an unauthorized EFT. Section 1005.2(m) explains an unauthorized EFT is any EFT from an 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 where an access device, such as a debit card, is used to access the funds as well as transfers where information, such as the account number, is used to access funds. 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. However, if the member is simply dissatisfied with a purchase she made, the transaction is not unauthorized.

The rule and staff commentary also provide a two examples of EFTs that are not considered unauthorized EFTs. First, an unauthorized EFT does not include a situation where the member acts, alone or with another person, with fraudulent intent. 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 would not be an unauthorized transfer because the member acted with fraudulent intent.

Second, if the member provides another person with authorization to make transfers from the account and they exceed the authority given by the member, those transfers are not unauthorized EFTs. However, once the member informs the credit union that this person no longer has authority to make transfers, then all future transfers are unauthorized EFTs. For example, if a member gives her daughter her debit card and PIN to purchase new shoes and the daughter instead buys a whole new wardrobe, the clothing purchases are not unauthorized. If the member informs the credit union her daughter no longer has authority to use her debit card then the daughter uses the card to purchase a new computer, the computer purchase is an unauthorized EFTs as the member has revoked the authority.

Error Resolution Procedures

When a member notifies a credit union of an unauthorized transfer, or other “error,” section 1005.11 requires the credit union to investigate and resolve the claim within a specified time period. The notice from the member must be received within 60 days after the periodic statement showing the error was sent. The notice needs to contain sufficient information to identify the member’s name and account number and provide known information about the type, date and amount of the alleged error.

A member’s notice can be provided orally or in writing. If the credit union chooses, it can require members to follow up an oral notice with a written notice within 10 business days. If the credit union chooses this additional requirement, it must inform the member of the requirement to send a written notice and provide the member with the proper address to use when sending the written notice. Importantly, the credit union cannot wait to begin its investigation until the written notice has been received. The investigation requirements discussed below begin when the member provides notice to the credit union - orally or in writing.

NAFCU NOTE
For more on the error resolution procedures, check out this NAFCU Compliance Monitor article (members only).

Investigation Requirements
Once a credit union has received a member’s notice of error, under section 1005.11(c) the credit union has 10 business days to complete the investigation. If a credit union is unable to complete its
investigation within 10 business days, the rule permits the credit union to take up to 45 days to conduct its investigation provided it does the following:

› Provisionally credits the member’s account with the amount of the alleged error within 10 business days from the date of the notice. If the credit union requires, but does not receive, written confirmation within 10 business days of an oral notice of error, provisional credit need not be provided;
› Notifies the member, within two business days, of the provisional credit in their account;
› Provides the member with full use of the provisionally credited funds during the investigation;
› Corrects any errors within one business day from determining the error occurred as described; and
› Notifies the member of the investigation results within three business days.

The 10 business days (for the initial investigation and providing provisional credit) is extended to 20 business days if the alleged error occurred within 30 calendar days of when the first deposit was made to the account. For the longer 45 day investigation process, the time period is extended to 90 days if the transaction was either: 1) not initiated in a state (i.e., foreign transactions); 2) a point-of-sale transaction using a debit card (including both PIN and signature as well as online and telephone transactions); or 3) occurred within 30 calendar days of when the first deposit was made to the account.

During the investigation, credit unions may ask the member for documentation or other information from the member. However, credit unions may not postpone the investigation nor deny a claim based solely on the member’s failure to provide such documentation. For example, although the credit union can request a copy of a police report the member has filed, it cannot require the member to provide a police report before it will begin or complete its investigation of the error. Similarly, the credit union cannot deny the member’s claim because a police report was not provided.

If an error has occurred, section 1005.11(c) requires the credit union to correct the error within one business day of determining the error occurred. This may include crediting the member’s account or making permanent the provisional credit. The credit union is also required to provide notice to the member within three business days of the conclusion of the investigation. The notice may be provided orally or in writing.

If the credit union’s investigation determines no error occurred or a different error occurred (such as a different amount or only one of the alleged transactions was an error), section 1005.11(d) requires the credit union to give written notice to the member. The notice must include the credit union’s findings and inform the member of their rights to request the documentation the credit union relied
upon. If provisional credit was provided, the notice must also identify the date and amount the member’s account will be debited.

**Member Liability**

Under section 1005.6, 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. 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 orally or in writing. As there are different notice requirements under the liability rules, a credit union may not be required to follow the error resolution procedures, but the liability rules will still apply.

As liability is dependent on when the member provides notice, a credit union may not use other factors to increase a member’s liability. For example, if a member’s negligence contributes to unauthorized transactions occurring on the account, the rules do not permit the credit union to use that fact to hold the member liable for more than what is allowed under Regulation E.

**Loss or Theft of an Access Device**

There are three separate liability levels that apply when an access device has been lost or stolen. “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.”

Section 1005.6(b)(1) explains the first level applies to unauthorized transfers occurring within two business days of when the member first learns of the loss or theft. Under this level, the member’s liability cannot exceed $50. The staff commentary explains the two business day timeframe depends on when the member “learns of the loss” not when the actual loss occurs. If the member provides notice to the credit union within the two business days, the other liability levels do not apply.

If the member does not notify the credit union within two business days of learning of the loss or theft, the second liability level will apply. Under this level, the member’s liability can reach up to $500 for the unauthorized transactions occurring after the two business days but still within 60 days after the periodic statement showing the unauthorized transfer was sent. Section 1005.6(b)(2) provides a two-part test for calculating the amount. The first part is the amount the member can be held liable for under the first liability level. The second part is the amount of the transactions that took place after the two business day period ended and before notification to the credit union, up to maximum of $500 for both parts.
Section 1005.6(b)(3) explains the third liability level applies to all transactions occurring more than 60 days after the periodic statement showing the unauthorized transfer was sent. If the member has failed to provide notice of the unauthorized transfers within the first 60 days after the periodic statement showing the unauthorized transfer was sent, then they can be held fully liable for the transactions occurring after the 60 days. This is in addition to the liability amount calculated under the first two levels.

**No Access Device Used**

If no access device was used as part of the unauthorized transaction, there are two levels of liability. In this case, liability is dependent on when the periodic statement showing the unauthorized transfer was sent to the member. The first level applies to all transfers occurring within the first 60 days after the periodic statement showing the unauthorized transfer was sent. Under this level, the member cannot be held liable for any amount. For the second level, section 1005.6(b)(3) indicates the member can be held fully liable for unauthorized transactions that occur more than 60 days after the periodic statement is sent and prior to notice to the credit union.

**MORE INFORMATION:** 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.
PROHIBITION ON REQUIRING ELECTRONIC PAYMENT OF LOANS

Often lost in the other requirements of Regulation E is the prohibition on requiring a member to repay a loan electronically to receive credit in section 1005.10(e). This means the credit union cannot create a product that forces the member to set up automatic electronic payments to repay the loan. However, the credit union can offer lower rates or fees on loans that have automatic repayment.

OVERDRAFT RULES FOR ATM AND ONE-TIME DEBIT CARD TRANSACTIONS

Section 1005.17 prevents a credit union from charging a fee for an “overdraft service” unless the member has opted-in for coverage. An “overdraft service” is “a service where a credit union assesses a fee for paying a transaction when the member “has insufficient or unavailable funds in the account.” The rule excludes lines of credit such including overdraft lines of credit covered by Regulation Z, and transfers between a member’s accounts such as a transfer from a savings account to a checking account. The overdraft fee prohibition only applies to ATM and one-time debit card transactions. It does not cover checks, ACH transactions, wire transfers or recurring debit card transactions (such as a monthly gym membership).

The credit union can still pay a transaction overdrawing a member’s account even if it does not have a member’s opt-in; however, it is not allowed to charge the member a fee for paying the transaction. A common situation is when a member swipes his or her card at a gas station and the merchant sends through a $1 authorization that is approved. The member fills up his or her gas tank and when the transaction later posts to the member’s account it takes the account negative. Without an opt-in from the member, the credit union may pay the transaction but is prohibited from charging a fee for doing so.

RESEARCH TIP: For a comprehensive review of the overdraft rules, see this Federal Reserve Consumer Compliance Outlook article, which also includes 24 Q&As. For a discussion of best practices, review the Interagency Guidance for Overdraft Programs.
**Opt-In Process**

For the credit union to be able to charge the member an overdraft fee for an ATM or one-time debit card transaction, the member must opt-in. Under section 1005.17(b)(1), the opt-in process consists of four parts:

- The credit union provides the member an opt-in notice in writing (or electronically if agreed), which describes the credit union’s overdraft program and discloses the potential fees;
- The credit union provides the member with a reasonable opportunity to provide the opt-in;
- The member provides affirmative consent (i.e., opt-in); and
- The credit union provides a written confirmation (or electronic if agreed) of the member’s consent, which must include information about the member’s ability to revoke their consent in the future.

Section 1005.17(d) requires the opt-in notice to follow [Model Form A-9](#). The notice must be segregated from other information. The credit union can require the member to decide at account opening whether they would like to opt-in for overdraft coverage; however, all four steps of the process must still be completed. Credit unions are not required to complete the opt-in process as part of opening a new account.

**Duration of Opt-in and Right to Revoke**

Under section 1005.17(f), a member's opt-in is effective until it is revoked by the member or the credit union ceases to offer the overdraft service. A member can opt-in to overdraft coverage for ATM and one-time debit card transactions at any time during the account relationship. The member’s right to revoke this opt-in also extends throughout the account relationship. The credit union must provide the same methods for a member to revoke as it does to allow a member to provide the initial opt-in consent.

For joint accounts, section 1005.17(e) explains any account owner can provide the opt-in to obtain overdraft coverage for ATM and one-time debit card transactions. The flip side of that coin is that the credit union must treat a revocation by any account owner as a revocation of the opt-in consent on the account. Thus, one joint owner could opt-in but have the consent revoked the next week by the other joint owner.
**Prohibition on Conditioning and Same Terms Requirement**

Section 1005.17(b) includes two separate provisions that require a credit union to treat members who do not opt-in the same as members who do opt-in. In other words, the credit union cannot punish members who have not agreed to overdraft coverage.

First, section 1005.17(b)(2) states the credit union cannot condition other overdraft services (such as for checks or ACH transactions) on whether the member has opted-in to overdraft coverage for ATM or one-time debit card transactions. Thus, the credit union cannot treat its overdraft program as an all or nothing program. The member must be able to obtain overdraft protection for checks, ACH and other transactions without being also required to opt-in for overdraft of ATM and one-time debit card transactions. Similarly, the credit union cannot refuse to pay checks or ACH transactions which overdraw the account solely because the member has not opted-in to overdraft coverage for ATM and one-time debit card transactions.

Second, section 1005.17(b)(3) states the credit union must offer the same account terms, conditions and features to members who do not opt-in as the credit union offers to those that do opt-in (aside from the actual overdraft coverage). For example, members who do not opt-in must receive the same dividend rate, same fees and the same card capabilities (such as both PIN and signature debit options). In short, all members must be treated similarly, without regard to whether a member has opted-in or not.

**EXAMPLE**

The staff commentary includes a detailed example: “For example, if an institution’s internal criteria would lead the institution to pay a check overdraft if the consumer had affirmatively consented to the institution’s overdraft service for ATM and one-time debit card transactions, it must also apply the same criteria in a consistent manner in determining whether to pay the check overdraft if the consumer has not opted in.”

Second, section 1005.17(b)(3) states the credit union must offer the same account terms, conditions and features to members who do not opt-in as the credit union offers to those that do opt-in (aside from the actual overdraft coverage). For example, members who do not opt-in must receive the same dividend rate, same fees and the same card capabilities (such as both PIN and signature debit options). In short, all members must be treated similarly, without regard to whether a member has opted-in or not.

**PREPAID ACCOUNTS**

Prepaid accounts have their own disclosure requirements and consumer protections under Regulation E. These types of accounts are still considered covered accounts, so the requirements discussed above for “accounts” still apply, including providing account opening disclosures and periodic statements.
and resolving errors. The rules for prepaid accounts discussed in this section apply in addition to Regulation E’s other requirements.

Section 1005.2(b)(3) explains a “prepaid account” includes the following:

› Employer-established payroll card accounts to which electronic transfers of salary or other employee compensation are made on a recurring basis;
› Government benefits accounts established by a government agency for distributing government benefits to a consumer electronically;
› Accounts marketed or labeled as “prepaid” and redeemable at multiple, unaffiliated merchants or usable at ATMs; or
› Accounts meeting the three following conditions:
   › Is either issued on a prepaid basis in a specified amount or is not issued on a prepaid basis but capable of being loaded with funds thereafter;
   › Primary function is to conduct transactions with multiple, unaffiliated merchants, at ATMs or for person-to-person (P2P) transfers; and
   › Is not a checking account, share draft account or negotiable order of withdrawal account.

The definition of a prepaid account is rather complex so the regulation and staff commentary provides additional explanations and examples that credit unions may find helpful. For example, the commentary explains what it means for a prepaid card to be marketed or labeled as “prepaid,” issued on a prepaid basis and capable of being loaded with funds. There are also examples applying the primary function test.

Section 1005.3(b)(3) provides some examples of products that are not prepaid accounts. These include certain gift certificates and gift cards; loyalty, award or promotional gift cards; general use prepaid cards marketed and labeled as a gift card or gift certificate; and health savings accounts. “Pass-through” accounts only capable of transferring but not holding funds are also not considered prepaid accounts. An example of a pass-through account would be a digital wallet that is only capable of storing a member’s payment credentials for other accounts but is incapable of storing any funds.

RESEARCH TIP: Because of the intricacies with the mere definition of a prepaid account, the CFPB created a six page flowchart to help credit unions determine whether a particular product meets the definition of prepaid account.
Disclosures

Section 1005.18 requires various types of disclosures for prepaid accounts both when the account is acquired and throughout the account relationship. The two main disclosure requirements, pre-acquisition and periodic statement disclosures, are discussed below but other required disclosures include: 1) account opening disclosures required under section 1005.7; 2) change in terms notices; 3) access device disclosures; and notices regarding unregistered prepaid accounts.

Pre-Acquisition Disclosures

Before a member acquires a prepaid account, section 1005.18(b) requires two disclosures: 1) a short form disclosure and 2) a long form disclosure. In general, a member acquires a prepaid account by purchasing, opening or choosing to be paid or receive wages via a prepaid account. There are specific content, placement and font size requirements for the short and long form disclosures. To assist credit unions in meeting these requirements, there are several model form disclosures that offer a safe harbor to credit unions that use them.

There are additional requirements for the disclosures if a prepaid account is acquired electronically, such as online or via a mobile app. Staff commentary explains credit unions must ensure the member is required to view the webpage displaying the pre-acquisition disclosures before accepting the prepaid account. Section 1005.18(b)(6)(i)(B) requires the electronic disclosures be viewable across all screen sizes, in a responsive form and using machine-readable text. For accounts acquired electronically, the pre-acquisition disclosures may be provided electronically without obtaining the consumer's consent in accordance with the E-SIGN Act.

Periodic Statement Disclosures

The periodic statement disclosures outlined in section 1005.9(b) apply to all prepaid accounts. Rather than sending a periodic statement each month or quarter for prepaid accounts, section 1005.18(c)(1) permits credit unions to provide alternative disclosures. To meet the alternative disclosure requirement, the rule requires credit unions to provide all of the following:

- The account balance via phone;
- An electronic history of account transactions for at least the past 12 months; and
- Upon request, a written history of account transactions for at least the past 24 months.

The electronic and written histories must include all of the information required for periodic statements under section 1005.9(b). The histories must also disclose the amount of any fee assessed against the account, not just those fees associated with EFTs. A total of all fees assessed against the account
must be included on each history for the previous calendar month and for the current calendar year to date.

MORE INFORMATION: The CFPB's Prepaid Rule webpage contains a number of helpful resources, including a coverage chart, small entity compliance guide and examination procedures.

Error Resolution Procedures and Liability

The error resolution procedures outlined in section 1005.11 and the liability limitations outlined in section 1005.6 apply to verified prepaid accounts. Section 1005.18(e)(3) provides additional information on when a prepaid account is considered unverified. Unverified accounts are fully exempt from the error resolution and liability rules.

For verified prepaid accounts, the rules require credit unions to investigate and resolve errors based on the same time periods stated in section 1005.11(c) when it receives timely notice of an error. Notice is timely when it is received within 60 days of when the credit union sent the periodic statement reflecting the error. Section 1005.18(e)(2) provides a modified notice time period for credit unions using the periodic statement alternative. Under the modified timeline, an error must be investigated if notice is received by the earlier of: 1) 60 days after the consumer accesses an electronic history that reflects the error, or 2) sixty days after the credit union sends a written history that reflects the error.

As an alternative to tracking the 60 days from accessing an electronic history or sending a written history, section 1005.18(e)(2)(ii) provides a safe harbor timeline. A credit union that investigates any error when notice is received within 120 days of the date the error was credited or debited to the account has properly complied with the rule.

NAFCU NOTE
This NAFCU Compliance Monitor article provides more details on requirements for prepaid accounts (member-only).

If the error is an unauthorized EFT on a verified prepaid account, the liability limitations in section 1005.6 still apply. If an access device was used, the first two liability levels that are based on the loss or theft of an access device remain unchanged. However, the third liability level, as well as the second
liability level for unauthorized EFTs where no access devices was used, that is based on when a periodic statement reflecting the unauthorized EFT is sent is modified for credit unions using the periodic statement alternative. Section 1005.18(e)(1) uses the same “earlier of” test described above for the investigation rules. The 120-day safe harbor also applies, which starts on the date the unauthorized EFT was debited to the account.

**REMITTANCE TRANSFERS**

Determining what is (and what is not) a remittance transfer is the first and arguably the most important step in determining your credit union’s compliance obligations under the remittance transfer regulations. Under section 1005.30, a remittance transfer is “the electronic transfer of funds requested by a sender to a designated recipient that is sent by a remittance transfer provider.” A “sender” is the person requesting the remittance transfer be sent to the designated recipient for personal, family or household purposes. A “designated recipient” is the person receiving the remittance transfer. The designated recipient must be located in a foreign country and can be either an individual or a business.

A “remittance transfer provider” is the person who provides remittance transfers in the normal course of business. To assist credit unions in determining whether they are providing remittance transfers in the normal course of business, section 1005.30(f)(2) provides a safe harbor. A credit union is not providing transfers in the normal course of business if it provided 100 or fewer transfers in the previous calendar year and provides 100 or fewer transfers in the current calendar year. If a credit union provided fewer than 100 transfers in each year, then it is not a remittance transfer provider and it would not have to comply with the remittance transfer regulations. The staff commentary provides further clarifications and guidance on these definitions.

**MORE INFORMATION:** In December 2019, the CFPB proposed to increase the remittance transfer provider threshold from 100 transfers to 500 transfers. The proposed rule would also permit remittance transfer providers to use estimates for the exchange rate and third-party fees in certain situations. For more, see NAFCU’s [Regulatory Alert](#).

**Disclosures**

Section 1005.31 requires credit unions who are remittance transfer providers to provide two types of disclosures to members requesting remittance transfers: 1) a pre-payment disclosure when the sender requests the remittance transfer but before payment is made and 2) a receipt when the sender
authorizes the payment. These two disclosures can be combined into a single disclosure as long as the credit union provides the member with proof of payment when the payment is made. Model disclosures can be found in Appendix A to Part 1005.

All disclosures must be provided in writing (or electronically if agreed) and in a retainable form unless the disclosures are provided via mobile app or text message to the extent permitted by section 1005.31(a)(5). Section 1005.31(e)(2) contains certain exceptions for transactions completed entirely by telephone, via mobile application or text message transactions. Credit unions conducting remittance transfers in this manner should closely review the regulation and staff commentary for additional information about the disclosure requirements.

Cancellation

Section 1005.34 contains the procedures for cancellation and refund of remittance transfers. A sender has the right to cancel a remittance transfer and receive a refund for up to 30 minutes after payment has been authorized for the remittance transfer, provided that:

- The request to cancel enables the provider to identify the sender’s name and address or telephone number and the particular transfer to be cancelled; and
- The transferred funds have not been picked up by the designated recipient or deposited into an account of the designated recipient.

This provision does not require that the credit union wait 30 minutes prior to accepting payment, nor does it require the credit union to wait 30 minutes to send the funds to the designated recipient. However, for operational reasons and to ensure that a member could cancel the remittance transfer and receive their refund, the credit union might delay transmittal until the expiration of the cancellation period.

MORE INFORMATION: The CFPB’s Remittance Transfer Rule webpage contains a number of helpful resources, including a small entity compliance guide, model forms and a list of the countries exempt from the rule.

Error Resolution Procedures

Section 1005.33 contains the procedures for resolving errors for remittance transfers. These procedures apply to any “error” which includes an incorrect amount paid by a sender, a computational error made by the credit union or the failure to make funds available to a designated recipient by the date
disclosed. An error does not include situations where the funds were sent to the wrong account because the sender provided the credit union with the wrong account number or institution identifier (such as a routing number).

Once a credit union has received notice of an error from the sender, section 1005.33(c) and (d) provide the specific procedures a credit union is required to follow. These include timely investigating and resolving the error. The specific resolution required will depend on the type of error asserted. Credit unions receiving a notice of error related to a remittance transfer should review the regulation and related staff commentary to ensure it is properly resolving any errors.