Protections under Regulation E

Regulation E, better known as the Electronic Fund Transfer Act (EFTA), outlines the rights, liabilities, and responsibilities of consumers that use electronic services covered under the EFTA and financial institutions that offer services covered under the EFTA.

Examples of EFTA covered electronic services

- ATM (Automated Teller Machine)
- ACH (Automated Clearing House)
- Debit Card Transactions (point-of-sale)

Examples of services **not** covered by EFTA

- Share Drafts (checks)
- Wire transfers
- Internal transfers between members' accounts initiated through a member's online banking account
- Internal transfer requests made via telephone conversation or in person with a FinancialEdge employee
- Internal transfers to a loan done through online banking, telephone conversion, or in person. Also includes internal recurring transfers that members have requested.

The above are just examples and are not an exausted list of EFTA covered and uncovered services. For more information on your rights, responsibilities, and liabilities under EFTA please review FinancialEdge's terms and conditions disclosure that is provided at account opening. You can also obtain a copy of the terms and conditions of your account on the Credit Union's website (www.financialedgeccu.org) by clicking on the disclosure link at the bottom right hand corner.

Additional Resources

www.ftc.gov
www.usa.gov
www.idtheft.gov
www.onguardonline.gov

FinancialEdge CU Contact Information

If you suspect or notice any suspicious account activity or experience any information security-related events with FinancialEdge's online banking you should immediately contact us at the following:

FinancialEdge Credit Union

Monday – Friday

LOBBY
9:00 am - 5:00 pm
DRIVE-THRU
(includes Member Contact Center & Loan-By-Phone)
8:00 am - 6:00 pm

Saturday

LOBBY
Closed

DRIVE-THRU
(includes Member Contact Center & Loan-By-Phone)
9:00 am - 12:30 pm

You can also go to one of 2 FinancialEdge branch locations to report suspicious account activity or discuss any security-related events within FinancialEdge's online banking.

1199 S Euclid Ave
Bay City, MI 48706

2601 Center Ave
Bay City, MI 48708

FinancialEdge
CREDIT UNION

Things you should know About Online Access Security

FinancialEdge Community Credit Union is always committed to ensuring the safety of our members' information and FinancialEdge's internet banking environment is no exception. With more and more members using internet banking, unscrupulous individuals are working harder than ever to find new ways to scam unsuspecting individuals. One of the best defenses against fraud is to remain educated on cyber-safety. FinancialEdge is dedicated to helping our members stay cyber-safe.

Tips on keeping yourself safe in the internet environment

1. **Keep Information Private.** Be extremely careful if you have to use a library or other public computer to access your account. Online fraudsters could have installed a keystroke logger to obtain your username, pin, and answers to security questions, and password.

   Fraudsters are known for masking emails and text messages to look like they come from a trusted sender. Do not send your account number or personal information via email or text messaging to anyone. Do not use a hyperlink that is located in an email to access FinancialEdge's online banking website and always ensure the the web address starts with https. FinancialEdge uses Website identification which is located to the right of the Credit Union's web address.

   If you receive a phone call from a person claiming to be a FECCU representative it is a good idea to ask for the representative's name and extension and inform the representative that you will call them right back. FECCU's call center will be able to direct your call to the extension given. DO NOT call the representative back on any number other than on a number that FinancialEdge has given you to call (989-892-6088) or is located in your local telephone book. A best practice is to always initiate contact yourself.

2. **Account Review.** FinancialEdge encourages members to log into their accounts regularly to review account activity, even if you have not done any recent transactions. Early detection is a key component to stopping fraud quickly. If there are any concerns, contact FinancialEdge immediately at 989-892-6088.

3. **Strong Password.** FinancialEdge encourages members to have a password that is at least 8 characters long with a mixture of upper and lower case letters, numbers, and special characters. Change your password regularly, do not give anyone your password or allow anyone else to use your password.

4. **Website Redirection.** If you click on a hyperlink that redirects you to a website that does not look like it is operated by FinancialEdge, use caution as the credit union may not operate it. FinancialEdge has pop up warnings on hyperlinks that we have placed on our website to inform you that you are being redirected to a site we do not operate. Use caution and contact FinancialEdge if you suspect there is a problem.

5. **Always Logoff.** Always logoff your FinancialEdge online banking session and DO NOT just close the browser.

6. **Assess your own risks.** FinancialEdge encourages every member to do their own risk assessment on their online banking security controls such as, but not limited to: Storage of online banking information (account number, password, pin, answers to security questions), and the type of antivirus protection you use on your computer.

FinancialEdge initiating contact with you

1. FinancialEdge's employees will **NEVER** call, email, or send you a text message asking for any of your electronic banking credentials. FinancialEdge may inquire about your electronic banking credentials if you initiate contact and express online banking problems.

2. Card fraud detection may contact you on behalf of FinancialEdge to verify unusual credit or debit card transactions. Card fraud detection will **NEVER** ask you for any of your electronic banking credentials. Card fraud detection will:

   - Introduce themselves to you as card fraud detection and that they are calling on behalf of FinancialEdge Community CU.
   - Card fraud detection *will* give you the last four digits of the card number they are contacting you about. **Do not** give anyone claiming to be card fraud detection your full card number, expiration date, three digit security number (located on the back of your card), or your full social security number.
   - Card fraud detection *will* ask you to verify the transaction(s) in question.
   - Card fraud detection *may* ask you for information about your address or last four of your social security number.
   - Card fraud detection will only ever call you about credit or debit card transactions.