

## **RE: Online Consumer Security**

EDSB is always looking for ways to make your banking experience more convenient, along with being safe and secure. Online banking, mobile banking and online bill pay are convenient ways for customers to manage financial matters and save time and money. In an effort to reduce threats and control fraud, EDSB is continually taking steps to improve controls which include keeping our customers informed on fraud matters. We also want to inform you of ways you can keep yourself safe online and limit online exposures.

### **Layered Security**

A good way to ensure your account remains safe from fraudulent activity is to use a layered security program. EDSB will continue to utilize up to date methods in layered security to ensure the online security of your accounts.

#### **Benefits of layering security include:**

- Strengthens your defense against fraud by providing multiple checkpoints to ensure transactions are authorized by the valid user.
- Assists in detecting suspicious activity, but strict procedures are required to ensure an effective response to each activity.
- The level of security (number of security layers) can be customized for the amount of risk.

#### **A layered security system includes:**

- Utilizing red herring questions. For example, questions with unusual answers that only you would know.
- Implementing a time limit to enter your security answers, so that if a hacker got into your account they would not have ample time to research an answer.
- Using a separate computer or device only for banking transactions and finances.
- Implementing the most current anti-virus and anti-spyware software programs.
- Changing your online banking password periodically.
- Email alerts to notify you of account changes.

### **Federal Regulation E**

EDSB also strives to keep our customers updated and educated. Regulation E is the federal regulation that addresses electronic fund transfers on consumer accounts.

#### **Regulation E provides protection for:**

- Point-of-sale transfers.
- ATM transfers.

- Direct deposits or withdrawals of funds.
- Transfers initiated by telephones.
- Transfers resulting from debit card transactions (whether or not initiated through an electronic terminal).

**Transactions excluded from Regulation E include:**

- Any transfer of funds originated by check, draft, or similar paper instrument (includes any payment made by check, draft, or similar paper instrument but that does not directly result in a debit or credit to a consumer's account).
- Any transfer of funds that guarantees payments or authorizes acceptance of a check, draft, or similar paper instrument but that does not directly result in a debit or credit to a consumer's account.
- Any transfer of funds through Fedwire or through a similar wire transfer system that is used primarily for transfers between financial institutions or between businesses.
- Any transfer of funds the primary purpose of which is the purchase or sale of a security or commodity. Some exceptions apply to this type of transaction.

**Your responsibilities under Regulation E**

Should you notice that there has been an error in an electronic fund transfer relating to your consumer account certain steps must be taken. Under Regulation E the consumer must:

- Write or call the financial institution immediately if possible.
- Must be no later than 60 days from the date of erroneous statement.
- Give name and account number.
- Explain why you believe there is an error, the type, dollar amount and date.
- May be required to send details of error in writing within 10 business days.

Through Regulation E you can be liable for unauthorized withdrawals if your EFT card is lost or stolen and you do not follow certain criteria. If you report your card missing to the institution before any transactions occur, you are not held responsible.

- Loss is limited to \$50 if you notify the institution within two business days.
- Loss could be up to \$500 if the institution is notified between 3 and 59 days.
- If loss is not reported within 60 business days you may risk unlimited loss on transfers made after the 60 day period – could lose all money in account plus maximum overdraft if any.

## Online and Mobile Banking

### Online and Mobile Banking Parameters:

- **Password Expiration:** You must change your password at least once every 12 months (you may change it more frequently).
- **Password Lock In:** You may change your password immediately after the password has been created or changed.
- **Password Warning:** You will receive a warning message 30 days before your password is scheduled to expire.
- **Variable Password Calculation:** Any time your password is reset you will never receive the same reset password.
- **Bank E-Mail on Failed Login:** Each time you exceed 3 failed login attempts an email will be sent to an EDSB personal banker as an alert.

### Password Restrictions:

- **Minimum Numbers:** You are required to have at least one number in your password.
- **Minimum Alpha:** You are required to have at least five letters in your password.
- **Password Reuse:** You must have at least 4 password changes before you may reuse a password.
- **Name and User ID Check:** This feature will prevent the use of the customer User ID, First Name, or Last Name as a password.
- **Password Restriction Words:** This feature prevents certain words from being used in your password, for example the word "password."

***EDSB will never contact you and request your online or mobile banking passwords or security questions. If we uncover fraudulent activity on your account we will contact you immediately and follow all necessary steps to secure your account.***

Many great resources exist to help you further understand how to protect your online and mobile banking experience, including:

[www.FTC.gov](http://www.FTC.gov)

[www.fsround.org](http://www.fsround.org) (Financial Services Roundtable)

## Securing your Personal Computer and Mobile Device

Online banking has evolved from strictly personal computers to include mobile banking through the use of handheld mobile devices, especially smart phones. The increased popularity and usage of mobile banking has led to new security concerns. These security concerns require additional safeguards and education for consumers. EDSB is dedicated to informing our customers about the importance of securing both their personal computers and mobile devices.

### **Secure Online and Mobile Banking Includes:**

- Securing your computer and mobile device through the use of passcodes to gain access. Studies show that a large percentage of people will lose their smart phone, and a majority of those people do not have their phone secured with a passcode. Fraudsters are eager to access personal information from lost or stolen cell phones, so this step is important for your protection.
- Utilizing the most up-to-date antivirus protection to safeguard against hackers. Online hackers and fraudsters are always devising new and creative ways to illegally access personal information. It is important to secure your mobile device with the most recent software protection.
  - Using available software patches is also an important step in securing your PC or mobile device with the most recent software protection. Ensure that the software patches are trustworthy before installing them.
- Securing home Wi-Fi networks with encryption, passwords, firewalls and updated security methods to keep others from gaining access to your personal and private information.
- Only using personally owned or controlled computers or access devices to access your accounts. Public computers (i.e. hotel lobbies, cafés, could contain malware or key logging software that would allow thieves to learn your username and passwords).
- Not storing sensitive information, passwords or other personal information, such as your mobile banking password or account numbers on your mobile device.
- Utilizing the password parameters and security related questions recommended by the Federal Financial Institutions Examination Council. Using complex passwords and selecting challenging security related questions can make it even more difficult for fraudsters to access your personal information.
  - It is recommended to use a combination of letters, numbers and special characters in your password that would be difficult for a fraudster guess.
  - The most effective passwords are comprised of a random sequence of letters and numbers that would only makes sense to you.

*If you notice suspicious account activity or have any questions regarding secured electronic funds transfers do not hesitate to call 563-556-7700 or email us at [CustomerService@edsb.com](mailto:CustomerService@edsb.com) for all resources available through EDSB.*