

## RE: Online Business Security

EDSB is always looking for ways to make your banking experience more convenient, along with being safe and secure. Online banking, mobile banking, remote deposit capture and online cash management are convenient ways for businesses to manage financial matters and save time and money. Online business transactions can involve ACH file origination, Remote Deposit Capture, online bill pay and frequent interbank wire transfers. Businesses have more frequent transactions and higher transaction amounts than personal accounts. These factors make it even more important that businesses take steps to control the level of risk to the business and the business customer.

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 to limit online exposure.

### Layered Security

One of the best ways to ensure your business 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. Only consumer accounts are covered by Regulation E. **Business accounts are not covered by Regulation E.** But Regulation E is explained here as it affects business owner's personal accounts and the accounts of their individual customers.

**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.

**Online and Mobile Banking**

EDSB is making changes to your online and mobile banking password set up too (business customers may use mobile banking, but are not able to use cash management services with it at this time). Please see below for updates:

**New Internet Banking Parameters:**

- **Password Expiration:** Previously you could use your password indefinitely. Now you must change your password at least once every 12 months.
- **Password Lock In:** You may change your password 3 days after the password has been created or changed. Previously this option was only available every 91 days.
- **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.

### **New 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.***

EDSB encourages online and mobile banking business customers to perform risk assessments and controls evaluations periodically to help ensure that your online and mobile banking experience is safe.

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 Business Computer and Mobile Device**

Online banking has evolved from strictly desktop 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 business 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 security 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.

## **Remote Deposit Capture**

### **Important information to insure Remote Deposit Capture operates effectively and securely for our RDC business customers:**

1. Your checks should be securely stored for 90 days. After 90 days the checks should be securely destroyed.
2. Only items with the correct business name matching the business account name shall be run through RDC.
3. RDC deposits should be transmitted no later than 5:00 p.m. for same day deposits.
4. No item shall be deposited through RDC more than once.
5. Passwords & access to RDC shall remain confidential and should not be shared with other employees. Only employees who need this information for their job function should have access and passwords to RDC.

*EDSB is making security a priority and looks forward to working with you going forward to strengthen your online and mobile banking. 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.*