Security Procedures to Enhance Your Online Protection

Cambridge Savings Bank's Business Online Banking platform is a powerful tool to help you manage and secure your company's financial assets and information. The security procedures described below are intended to help protect you against online threats and are reflected in your Payment Order Agreement with us. Please review the following information carefully.

Additionally, if you do not currently have adequate controls in place, incorporating these "best practices" into your internal policies and procedures will help to protect your critical information while utilizing our Business Online Banking technology.

Multi-Factor Authentication

User credentials uniquely identify each person who uses the banking platform. The intent of authentication is unequivocal verification of the user's claimed identity.

The main factors used for authentication are:

- Something the user knows (passwords)
- Something the user has (One Time Passcode (OTP)/token)

When an authentication system uses more than one factor of authentication, the system has a higher assurance that the user authenticating is the correct and intended user of the account. If a fraudster knows the username and password for an account, but does not possess the OTP/token, they are not able to authenticate.

Multi-Factor Authentication mitigates compromised user credentials, password reset attacks, phishing attacks, key logger attacks, and some Man-in-the-Middle attacks.

Passwords.

A well chosen password has two important characteristics; it should be easy to remember, and hard to guess. Passwords should be changed at least every 60 days in order to combat the possibility of undetected password compromise.

Passwords should:

• Be no fewer than 8 or greater than 24 characters in length; 14 characters or longer is ideal
• Combine letters (uppercase and lowercase), numbers, and symbols

Passwords should not include:

- Your name or the name of a family member or pet
- Social Security, account, or phone numbers
- Any part of your address
- Anybody's birth date
- Sequential numbers ("12345678") or letters ("abcdefgh")

Passwords should never be written down anywhere. Passwords should never be shared with anyone.

csb Cambridge SAVINGS BANK

Dual Control

Dual control is an important measure to reduce fraud risk and is particularly critical in regard to the authorization of Wire Transfer and ACH payment orders. For example, with dual control, one user has permission to initiate a funds transfer, while a second user must approve the transfer. By separating the capabilities, you prevent a single user from transferring funds without oversight or a fraudster from moving funds with a single set of credentials.

Setting Limits

Setting limits is another measure that can help to mitigate fraud risk. Establishing limits to the dollar amount of Wire Transfer and ACH payment orders each user may process will reduce exposure to loss in a single transaction. Limits should be set based on need for customary transaction volume.

Activity Reporting

Activity Reporting should be reviewed on a daily basis to identify any suspicious or unusual activities. The activity may include transactions, logins and the associated IP addresses, and the time these activities occurred. Ideally, this review should be conducted by someone other than those who originate transactions.

Alerts

Alerts offer another method to monitor activity on your account.

Balance Alerts allow parameters to be set to generate an email alert if balances rise above or fall below a designated limit.

ACH and Wire Transfer Alerts notify you when there's an ACH or Wire Transfer (Money Transfer) that requires your approval. You can also receive alerts notifying you when a Money Transfer is completed (i.e. sent to the Bank for processing). These alerts provide you with information about transactions that may require your attention, and also help alert you to any unauthorized transactions before it's completed.

Questions

If you have any questions or concerns regarding your online security, please call our Customer Contact Center at **888.418.5626,** Monday-Friday 8am-6pm, Saturday 9am-3pm, or Sunday 10am-3pm.