Internet Security

The Internet has changed the way your credit union does business. Internet banking provides convenient access to information and the ability to perform transactions from home, work or other locations. It is important to be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or a virus in a very short period of time.

What we are doing to protect your security

We take many precautions to protect the online banking environment and ensure your information is safe. Our online services offer you the best security currently available in the online environment so that your personal and financial information is protected while in transit between your computer and our server. This is done through the use of industry standard security techniques such as encryption. Encryption ensures that information cannot be read in transit or changed by scrambling the data using a complex mathematical formula. Some browsers can create a more secure channel than others, owing to the 'strength' of their encryption. We use only the strongest channel available - referred to as 128-bit SSL (Secure Socket Layer). If you have a browser that only supports 'weaker' encryption such as 40-bit or 56-bit SSL, you should upgrade your browser before using our online services. The longer and more complex the 'key' is, the stronger the encryption. The 40 and 128 refer to the length of the key. Since 128 is longer, than 40, it is more secure.

We utilize multi-factor authentication to access your accounts. This requires a PIN (Personal Identification Number) selected by you, entry of a random access code, and answering of a security question selected by you. In addition, you select a unique security key to ensure you are conducting transactions on Dover Federal's site as opposed to a fraudulent site. To help you protect your information, your online banking session will end automatically if there has been no activity for 10 minutes.

Access to our databases is strictly managed and systems are in place to ensure security is not breached, including the physical security of our computer hardware and communications.

Protecting Your Personal Identification Number (PIN)

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected.

In order for us to ensure that *only* you are accessing your accounts, we need a unique way of knowing that it's you. Just as the key to your home protects unwanted entry, the online banking 'key'—your Personal Identification Number (PIN)—ensures that only you can access your accounts.

It is your responsibility to ensure that your 'key' to the online banking section of our website is protected. Please observe the following security practices:

- Select a PIN that is easy for you to remember but difficult for others to guess. Your PIN should be the maximum allowed of 8 digits.

- Do not select a part of your ATM or Debit Card PIN or another password.

- Keep your PIN confidential and do not share it with anyone other than joint owners of your membership.

- Do not write your PIN down or store it in a file on your computer.

- Never disclose your PIN in a voice or email, and do not disclose it over the phone.

- Ensure no one observes you typing in your PIN. Our Internet Banking system allows you to 'hide' the text from appearing on the screen while you are typing.

- Change your PIN on a regular basis. We suggest every 90–120 days.

Protecting Your Computer

We have provided a secure channel for our members to communicate with us. Once the information has reached your computer, it's up to you to protect it. To protect your information, you should:

- **Never leave your computer unattended** while using our online banking services.

- **Always exit the site using the Logout button** and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.

- **Secure or erase files** stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to 'empty' the cache.

- **Disable automatic password-save features** in the browsers and software you use to access the Internet.

- **Install and use a quality anti-virus program.** As new viruses are created each and every day, be sure to update your anti-virus program often. It is recommended you update anti-virus definitions weekly. Scan all download files, programs, disks and attachments and only accept files and programs from a trusted source.

- **Install and use a personal firewall** on your computer to ensure others cannot access your computer through the Internet.

- **Install new security patches** as soon as your operating system and Internet browser manufacturers make them available.

- **Install an anti-spyware program** and check your computer regularly.

Protecting Your Information When Using A Public Computer

You should be extra vigilant when using publicly available computers. Even if you adopt the tips above to protect your information, you need to bear in mind that even benign programs, like popular desktop search programs, can pose a security risk. Certain programs, such as Google Desktop, cache items that you have viewed so you - or potentially, an unwelcome third party - can easily search and find those pages later again.

If you come across a program like this when you are using a public computer, you can adjust the search program preferences so it does not store secure pages you wish to view. If you forgot to adjust the preferences before

banking online, you can remove the stored items via the Google Desktop results page by clicking on the Remove items link.

To learn more about browser security, please visit the Microsoft web site. To ensure a safe and secure Internet session, only visit reputable sites. If you visit any questionable web site beforehand, we recommend you close your browser and restart it before proceeding to use our online banking services.

Fraud: Recognize it. Report it. Stop it.

Electronic identity theft can occur when you respond to a fraudulent email that asks for your personal banking information. Armed with this information, a person may be able to access your accounts or establish credit, pay for items or borrow money using your name. You can help protect yourself from electronic identity theft by following some simple precautions.

Safety Precautions for Internet Banking

- The easiest way to tell if an email is fraudulent is to bear in mind that we will never ask you for your personal passwords, personal information numbers or login information in an email.

- When banking online, check the address of any pages that ask you to enter personal account information. In the toolbar at the top of the page any legitimate Internet banking web site will begin with 'https' to indicate that the page is secure.

- Look for the padlock found in the lower right corner of your screen. If the page is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.

- Type in our web address yourself to ensure you are transacting with our server.

- Check your Dover Federal statements regularly to ensure that all transactions are legitimate.