ONLINE SECURITY PROMISE

I. Overview

The Internet is a rapidly changing marketplace with a wide variety of goods and services available online. Although financial institutions agree on the merits of Internet financial services, some consumers are concerned about security.

This online service is built on a foundation of stringent security policies, rigorously tested technologies, and a highly trained and experienced staff. Our combination of Internet expertise and in-depth knowledge and experience in the financial services industry provide a secure solution to consumer concerns. You may rest easy knowing that financial information will be protected with state-of-the-art security every step of the way.

II. Secure Systems - Technology, Policies, and People

Secure systems are a combination of technology, policies, and people. Our system is designed with security as a dynamic feature of the product, not an afterthought or add-on. The result is an architecture that utilizes a multi-layered approach to information security, providing safeguards and privacy throughout the process.

This architecture offers client-server authentication, data integrity, complete transactional privacy, and above all, resistance to all forms of "hacking" attempts. Layered security means that rather than relying on a single security measure, layers of technology are utilized within the security architecture to distance the potential "hacker" as far as possible from the core of sensitive information and resources.

III. Security Architecture - Multi-layered Approach

Every financial transaction uses multiple layers of security and every layer adds a different technology resulting in a trusted system that is monitored at all times. There are five basic layers.

A. The Web Browser Layer

The first layer of online financial security is the Transport Layer Security (TLS) encryption between your browser and the Web Servers. TLS is the industry standard that provides secure access to online financial services from anywhere on the Internet using any current Internet browser.

TLS provides a secure channel for data transmission over the Internet. It allows for the transfer of digital signatures to authenticate users and provides message integrity, ensuring that your data cannot be altered en route. Browsers can also display a certificate to the user about the source of a secure transmission. This assures Internet users that they are communicating with the financial institution's service provider and not a third party trying to intercept the transaction on the Internet.

Encryption changes everything that travels across the Internet during your online session (including your password, your bank statement, and instructions to pay a bill) into a string of unrecognizable numbers. Both our servers and the browser you use to surf the Web understand the mathematical formulas, called algorithms that turn your financial information into numeric code, and back again to meaningful information. These algorithms serve as the locks and keys of your account information. While the destination computer and your browser can easily translate this code back to meaningful language, this process is an overwhelming, almost impossible task for unauthorized intruders.

There are two types of encryption commonly in use "domestic-grade" or 128-bit encryption and "international-grade" or 40-bit encryption. The difference between these two types of encryption is strictly one of capability. 128-bit encryption is stronger than international-grade encryption. Using 128-bit encryption, means there are 300,000,000,000,000,000,000,000,000 (a three followed by 26 zeroes) times as many key combinations as there are for 40-bit encryption. That means a computer would require exponentially more processing power than for 40-bit encryption to find the correct key.

We require the use of at least 128-bit encryption for all financial transactions to provide the best security possible. In addition to browser encryption, there is server encryption for users who log in with a browser that has only 40-bit encryption. The server will accept the message and start a 128-bit encrypted session from the server end. This ensures that all your transactions have the strongest level of encryption.

To start a transaction, you enter an address in the browser to send a secure message that is encrypted by TLS to a server. The server responds by checking to see who you are (this is called authentication), comparing your encrypted User ID and Password against an encoded list, and starting the session encryption. If, for any reason, the secure session link is broken, the online session automatically terminates.

B. The Firewall Layer

An Internet firewall provides a point of defense. This is a controlled and audited access path to services from inside and outside the organization's private network. The firewall provides a second layer of security by selectively permitting or blocking traffic between the Internet and the protected network. Specifically, the firewall shields the server from any unauthorized Internet traffic. Only messages addressed to the secure server can pass through the firewall. All other traffic from the Internet is rejected. To pass through this checkpoint, your browser must know the protocol to use. In other words, the language to speak that will allow it to obtain authorized information, but only from designated systems. The firewall creates extensive logs of all network traffic providing centralized auditing and security monitoring.

C. The internal Network Layer

The third layer of security is the internal network which prevents unauthorized users from accessing any transaction data from the Internet by means of physical and logical access controls. Transaction processing systems are not physically connected to the Internet. Once your transactions have been accepted by the server, they are carried over the proven secure network

that financial institutions have been using for decades. The entire process from the financial institution to you is as secure as possible.

D. The People Layer

The fourth layer of security is people. Internet security does not rely on technology alone. Without everyone's participation, all the security systems and technology in the world are worthless. Users must treat the User ID and Password for online accounts with the same care as an ATM or Credit Card and PIN. In addition, users must make sure that no one is physically watching when they enter their password. If you are logged into the service, be sure to logout and exit the browser when you leave the computer unattended. You should also take standard precautions to keep your system clean and free from viruses that could be used to capture password keystrokes and financial information.

We don't view security as something that is set up once and left alone. Your online service provider constantly monitors the security system to be sure that your information is safe and secure. Any attempt to break into the system will be observed.

New advances in security technology are happening daily. As an active member of the Internet financial services community, we are continuously reviewing and enhancing security architecture to ensure that it provides the highest level of privacy and safety for you.

E. Multi-Factor Authentication Layer

The fifth layer of security involves multi-factor authentication (MFA). MFA is a security feature implemented to provide another layer of authentication when remotely accessing your financial information. If anything unusual is found during an attempt to log into your account, the person trying to gain access to the account will be "challenged". Depending on the system that is trying to be accessed, the challenge will vary. For instance, the person may be required to answer questions about your background or a one-time PIN may be sent to your email. If the person fails to complete this challenge, your account will be locked until we can speak directly to you. At that time, access to your account will be unlocked and you can proceed to log in. If these attempts were not authorized, we will suggest that you change the username and password used to gain access to this account.

IV. Member Security

We want your online banking experience to be enjoyable and safe. That's why we use at least 128-bit transport layer security (TLS) encryption, constantly updated and monitored systems along with multiple security layers and procedures. We also want to make you aware of several straightforward security tips to keep in mind:

- Use a strong password. Choose passwords that are difficult for others to guess and use a different password for each of your online accounts.
- Change your Online Banking Passwords often. You can do this quickly and easily by signing on and going to the profile area.
- Leave suspicious sites. If you suspect that a website is not what it purports to be, leave the site immediately. Do not follow any of the instructions it presents. For Microsoft Internet Explorer

(IE) users setting your browser security setting to "high," a level that makes it more difficult to interact with some Web sites is also recommended.

- Be alert for scam emails. These may appear to come from a trusted business or friend, but actually are designed to trick you into downloading a virus or linking to a fraudulent website and disclosing sensitive information.
- Don't reply to any email that requests your personal information. Be very suspicious of any email from a business or person that asks for your password, Social Security number, or other highly sensitive information and/or one that sends you personal information and asks you to update or confirm it.
- Open emails only when you know the sender. Be especially careful about opening an email with an attachment. We advise that you shouldn't open attachments unless you are confident that you can trust the source.
- Be careful before clicking on a link contained in an email or other message. The link may not be trustworthy.
- Do not send sensitive personal or financial information unless it is encrypted on a secure website. Regular emails are not encrypted and are more like sending a post card. Look for the padlock symbol to ensure that the site is running in secure mode before you enter confidential personal information.
- Don't take anything for granted and only do business with companies you know and trust. Always keep in mind that forging emails and creating phony "look alike" websites designed to trick consumers and collect their personal information is not difficult. Make sure that websites on which you transact business post privacy and security statements, and review them carefully.
- Make sure your home computer has the most current anti-virus software. Anti-virus software needs frequent updates to guard against new viruses. We recommend that you use a program that automatically upgrades your virus protection on a regular basis. If you currently do not have this automatic upgrade feature, make sure you update your virus detection program weekly and when you hear of a new virus. If your anti-virus product doesn't include spyware protection, we recommend that you install a reputable spyware detection product as well.
- Install a personal firewall to help prevent unauthorized access to your home computer. This is especially important if you connect to the internet via a cable modem or a digital subscriber line (DSL) modem.
- When your computer is not in use, shut it down or disconnect it from the Internet.
- Act quickly if you suspect fraud. If you believe someone is trying to commit fraud and/or if you think you may have provided personal or account information in response to a fraudulent email or website, report the incident immediately, change your passwords and monitor your account activity frequently.