Recommended Financial and Information Security Practices for Online Banking

Use Personal Financial Information and Financial Services Passwords Only in Secure Transactions

• Personal financial information (such as names in combination with Social Security Numbers, account numbers, and credit or debit card numbers) and passwords for financial services (such as online and mobile banking / payments, and person-to-person payments) should only be used in secure transactions using the practices described here.
• Personal financial information and passwords for financial services should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.
• If you provide financial information and passwords for financial services in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages, you should change your passwords as quickly as possible.

Use Strong Passwords in All Systems that Require Passwords

• Passwords should use the maximum allowable number and type of characters (such as upper and lower case letters, numbers and symbols) and should not contain predictable terms or numbers.
• A different password should be used for each commercial and financial services website.
• Passwords that are written down or otherwise recorded should not be placed in visible or unsecured locations.

Approach Applications and Links on All Devices and Delivery Channels with Caution

• Approach all applications and links on all devices (such as personal computers, tablets and cell phones) and delivery channels (such as email, text messages and social media sites) with caution, as cybercriminals often use applications and links as the first step in installing malicious software on devices with which fraudulent acts can be enabled.
• Take steps to verify that applications and links posted on social media sites correspond to legitimate websites, and that they have been posted by individuals who are known and trusted.

Use Computers and Online Banking, Bill Payment and Shopping Securely

• Antivirus protection and scanning software that has been reviewed and rated as satisfactory by independent analysts should be installed, updated and utilized as recommended. In addition:
• If the security software can update automatically, set it to do so.
• If the security software cannot update automatically, update it after each login.
• If viruses (also referred to as “malicious software” or “malware”) are detected, the recommendations provided by the antivirus program should be followed promptly.
• Operating system software updates (also referred to as “patches”) should be accepted, downloaded, installed and run promptly, and as recommended.
• Personal financial information should never be sent by email in an unencrypted state. An email solution that encrypts messages between financial institutions and their customers should be utilized.
• Financial transactions that are conducted on websites should be conducted on secure websites only. An indicator of a secure website is a URL that begins with “https” in the address,

the “s” standing for “secure.” The “https” prefix should be on every page of websites used to conduct transactions, in addition to the sign-in page.
Privacy policies should be easily found and understood. If the privacy policy is not easily found and understood, then consider conducting business elsewhere. Privacy policies provided by financial institutions in connection with financial services are required to offer consumers a clear method to “opt out” of certain types of information sharing if the institution engages in them.
• Most Wi-Fi networks do not encrypt information and are not secure. Some use encryption and are more secure, WPA being common and WPA2 the strongest. However, if any Wi-Fi network is to be used, a virtual private network (VPN) should be established and used to encrypt communications. VPN encryption applies all the way from the user’s PC to the host computer, regardless of the type of network used. The encryption methods used by VPN are stronger than WEP and WPA.
• Unfamiliar or suspicious emails, text messages, instant messages, phone calls, websites and social media solicitations that request personal financial information should be deleted immediately. They should not be replied to or forwarded, and any links that they contain should not be opened.
• Options to “Remember me” on websites where transactions are conducted should not be used.
• Computer workstations and laptops should be logged off, and preferably not left on, when the user steps away.
• Computer workstations and laptops should be set to logoff automatically after no more than two minutes of non-use, with a password required to log back in.
• Computer workstations, laptops and external storage devices such as USB drives and storage discs should be physically secured with locks (such as with a cable lock or in a locked drawer) when not in use.
• Computers that are no longer in use should have hard drives removed and shredded, or a software program that wipes and eliminates all data from their hard drives should be used, following DOD5220 standards for data sanitization.

Use Mobile Phones, Mobile Banking and Mobile Payments Securely
• Mobile phone applications, text messages, instant messages and calls from unfamiliar or suspicious sources that request personal financial information and passwords should be declined and, when appropriate, promptly deleted, and not replied to or forwarded. Any links they contain should not be opened.
• Each mobile phone and mobile phone application should be assigned a different password with the maximum allowable number and type of characters.
• Mobile phones should be set to logoff automatically after no more than two minutes of non-use, with a password required to log back into the phone.
• Mobile phones should be locked up when not in use and not left in visible, unsecured locations.
• Lost or stolen phones should be reported to the carrier promptly.

Use ATM, Credit, Debit and Prepaid Cards Securely
• Cards should be signed as soon as they arrive.
• Card numbers should only be used in secure transactions and should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.
• If conducted on websites, card transactions should be conducted only on secure websites. An indicator of a secure website is a URL that begins with “https” in the address, the “s” standing for “secure.” The “https” prefix should be on every page of websites used to conduct transactions, in addition to the sign-in page.

• Options to “Remember my card number” on websites where transactions are conducted should not be used.
• Cards should not be left in visible or unsecured locations.
• Lost or stolen cards should be promptly reported to the card issuer.
• Cards that are unused, have been canceled or have been replaced by a new card should be securely eliminated, for example by cutting them into small pieces so they cannot be read.

Use Checks Securely
• Checks should not have Social Security Numbers or driver’s license numbers printed or written on them.
• Checks should not be left visible in unsecured locations.
• Checks that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.
• Checks that are tamper-resistant are available at certain financial institutions. These checks include security features such as chemically sensitive paper to deter alterations.

Use Statements and E-Statements, Bills and E-Bills, and Transaction Receipts Securely
• Statements, e-statements, bills and e-bills should be reviewed promptly upon receipt to verify that all transactions were made by authorized parties; any transactions made by unauthorized parties should be reported to the appropriate financial institution, card issuer or biller.
• Transaction receipts should be saved and compared to statements to ensure that unauthorized charges have not been added. Any transactions made by unauthorized parties should be reported to the appropriate financial institution, card issuer or biller.
• Incorrect transaction receipts should be voided.
• Blank transaction receipts should not be signed. Draw a line through any blank spaces above the total on any transaction receipt that is to be signed.
• Statements, bills and transaction receipts that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.
• Financial institutions, card issuers and billers should be notified in advance of a change of address.

Use Social Media Securely
• The highest available level of privacy and security settings should be selected and activated on any social media site.
• No information that can be used to compromise information security should be viewable on any social media site. Such information includes the names of financial institutions, card companies, commerce websites, Internet service providers, utilities and wireless carriers with which you have accounts.
• Accept only known and trusted individuals into your social network.
• Do not allow social media sites to scan your address book.

Monitor Credit Accounts
• Credit accounts and reports should be monitored regularly. Any unauthorized or suspicious activity should be reported promptly to the appropriate financial institution, card issuer, local law enforcement agency and the Federal Trade Commission (877-438-4338, or online at www.consumer.gov).
• As a precaution, you may choose to place a fraud alert on your credit file. A fraud alert will notify you before unauthorized third parties open new accounts in your name or charge existing accounts in your name. This can be done at no charge to you. To receive fraud alerts, contact Equifax® (800-525-6285), Experian® (888-397-3742) or TransUnion® (800-680-7289).