Online Privacy and Security Policy

(Rev. 12/18)

How We Protect You

This New Century Bank Online Security and Privacy Policy explains how we may collect information from you online when you visit our website. Our commitment to protect your information and your privacy extends to your online banking. While our privacy policies are the same, whether you are online or not, we have extra measures in place to protect your privacy when you bank online with us.

How we handle information about you when you visit our website will depend on what you do when visiting the site.

Visiting

If you visit our website to read information and do not use any of our online services, then we collect and store only the name of the domain from which you access the Internet, the date and time you access our website and the Internet address of the website from which you linked directly to our website. We may record the "IP address" assigned to you by your internet service provider as part of this process. We use the information we collect to measure the number of visitors to the different sections of our site, and to help us make our website more useful to visitors.

Using Services

When you visit our website, or use our electronic banking services, there may also be times when you are asked to provide information about yourself that is personally identifiable ("Personal Information"). This may include any of the following:

- your first, middle and last name,
- your home or other physical address (including street name and name of a city ortown),
- your e-mail address,
- a telephone number,
- social security number,
- account number,
- date of birth,
- mother's maiden name, and
- password or any other identifier that permits physical or onlinecontact with you.

Personal Information might be needed or requested from you so you can register for banking or other services, or to fill out our forms or applications for services, for special promotions or contests, to accomplish transactions you request (such as bill payment or other banking services), or send you important information regarding the services, changes, to this Policy and/or other similar administrative information. This may result in sharing of Personal Information with third parties (such as data processors or service bureaus) as part of servicing your accounts or transactions.

There may be a need for you to contact us to make changes to your Personal Information. When you contact us through our website or online banking, a bank representative will contact you shortly after to ensure the validity of the request. Upon verifying your identity and confirmation of the request, the changes will be documented within the appropriate account forms to be signed by you. No changes will be made until the fully executed account forms have been received by the Bank.

When you supply us with your postal or e-mail address or telephone number online, you may receive periodic mailings or telephone contact from us with information on new products, services or upcoming events. If you do not wish to receive such mailings or contact, please call us or write us at the telephone number or address shown on your account statement. Please provide us with your exact name, street, and e-mail address. Even if you make this choice, we may still send you e-mail to deliver your statements (which may include marketing materials) or give your account-related notices or other information.

Cookies

There is a technology called "cookies" that can collect, store, and sometimes track information. A cookie is a small data file that can be placed on your hard drive when you visit certain websites. We use cookies to store your preference information on the use of our site and to facilitate access to restricted web pages during a single online session. A session cookie (or 'session variable') is used to authenticate your login information.

While you are logged on viewing your account information or conducting online transactions with us, we recommend that you do not access other websites during your online session. Always exit from your online session with us before moving to or accessing other websites and prior to turning off your computer.

Some browsers allow you to reject cookies. However, if you set your browser to reject cookies, you may find that you are unable to conduct your online transactions with us. If you choose to NOT accept cookies while accessing web pages on the Internet, we suggest that you enable acceptance of cookies when you are logged onto your online session with us. For detailed instructions on enabling and disabling cookies, refer to your web browser's online HELP menu or user manual.

Our Site does not process or respond to "do not track" requests or other similar web browser mechanisms, which enable users to indicate an opt-out preference regarding the collection of Personal Identifiable Information. By using our Site, you acknowledge and agree that anonymous information may be collected. By completing a form or other request for information, you agree to the collection of this information. Please note that industry standards are currently evolving, and we may not separately respond to or take any action with respect to a "do not track" configuration set in your internet browser.

E-Mail

You may also decide to send us information that personally identifies you, for example, in an electronic mail (e-mail) message. We will use that information to respond to the inquiry and provide accurate information in response to questions. We preserve your e-mail address, our response, and the original content of your e-mail for a period, so we can efficiently handle any follow-up questions you may have. We also do this for legal, regulatory and account servicing requirements.

If you visit our website or engage in any online services that we offer, then we may collect and store these categories of Personal Information. We will not share the Personal Information you provide us at our website or by e-mail, except as described below. The Personal Information we obtain from you is stored with us if it is to be used on an on-going basis.

Security Procedures

We want you to use our website with confidence, knowing that the information you submit to us is secure. The encryption strength varies depending on the browser you are using; however, most current browsers offer 128-bit encryption. Additionally, many browsers display a secured lock symbol to indicate a secure connection. Emails that you may send to us outside our online banking service may not be secure unless we advise you that security measures will be in place prior to your transmitting the information. For that reason, we ask that you do not send confidential information such as social security or account numbers to us through an unsecured email.

For clients, when your login to Internet Banking the Secured Socket Layer (SSL) protocol is used to establish a secure and encrypted session with our service providers. This encryption is designed to ensure the privacy and integrity of the information exchanged. You can tell whether your browser is in secure mode by looking for the secured lock symbol on your browser window. To obtain details about the encryption, position your mouse over a blank area on your screen and right-click to select "properties" information about the page being viewed (Note: the title for "properties" will vary by browser). The properties or page information section will indicate the encryption strength being used to view the secure page.

We have implemented multifactor and multilayer authentication, in addition to online banking user security, which requires multiple pieces of information to validate identity while ensuring compliance with regulatory requirements and Federal Financial Institutions Examination Council (FFIEC) recommendations. Multifactor Authentication automatically monitors accounts for unusual activity based on account history and requires customers to verify their identity by answering pre-selected challenge questions. Token solutions for online banking provide hacker- resistant multi-factor authentication protection for online transactions. Based on time- synchronization technology, this authentication device solution generates a simple, one-time authentication code that changes at the push of a button. Clients are thus able to access their account online by entering the token code following their existing login credentials – resulting in a unique, one-time-use passcode that positively authenticates the client and only permits access to online banking if the code isvalidated.

Links

We are not responsible for practices employed by websites of other companies linked to or from our site, nor the information or content contained therein. We cannot, and do not, make any representations about the security, practices and policies of these companies, and are not responsible in any way for how these companies use cookies or any information you provide to them. This remains true even where the linked site appears within the parameters or window/frame of our website. Often, links to other websites are provided solely as pointers to information on topics that may be useful to users of our site. Please remember that when you use a link to go from our website to another web site, our Online Privacy and Security Policy is no longer in effect. Your interaction on any other website, including websites which have a link to our site, is subject to that website's own rules and policies. Please read those rules and policies before proceeding.

Changes to the Online Privacy and Security Policy

From time to time, we may make changes to this Policy in order to accommodate new technologies, industry practices, regulatory requirements or for other purposes. We encourage you to review the Policy periodically to ensure that you understand how we collect, use and share information through the Services. If we do make changes to the Policy, we will also update the "Revision Date" posted at the top of the Policy.

Privacy

New Century Bank protects and values your privacy. The Bank thanks you for the trust you place in us. We want you to know that the information you share with us is treated with care. In this Online Privacy and Security Policy, we refer to the term "Personal Information", which includes:

I. information you provide to us to obtain a financial product or service;
II. information resulting from any transaction involving a financial product or service between you and the Bank; or,
III. information we obtain in connection with providing a financial product or service to you.

Children's Privacy

Our Site is not intended for use by children under the age of 13. We do not knowingly market to, nor solicit data from children.

Reporting Fraud

Think You Are a Victim of Fraud?

Reporting Suspicious Information - are you receiving suspicious information such as e-mails requesting your online banking User Name or password, ATM PIN, or telling you your Debit Card has been deactivated? Have you received any other security notices or information you think may be suspicious?

Please contact us at (785) 527-2772 to report such information.

Scams

The following scams are commonly reported in today's environment:

"Pharming"

"Pharming" (pronounced "farming") is another form of online fraud, very similar to phishing (see below). "Pharmers" set up bogus websites to obtain confidential information and perpetrate online scams. However, pharming scams are much more difficult to detect than phishing scams because criminals are not dependent upon the victim accepting a "bait" email. Instead, rather than relying on users clicking an enticing link in a fake email message, pharmers redirect victims to a bogus website even when they type the correct website address in their browser. The criminal then proceeds to load spyware and adware on the victim's computer to collect personal information and use it to commit fraud or other crimes.

"Phishing"

"Phishing" (pronounced "fishing") is a criminal tool employing both social engineering and technical subterfuge to steal a person's personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate agencies and businesses to lead consumers to counterfeit Web sites designed to trick recipients into divulging financial data such as user names and passwords. Technical subterfuge schemes plant crime ware onto personal computers to steal credentials directly, often using systems to intercept consumers online account user names and passwords and to corrupt local navigational infrastructures to misdirect consumers to counterfeit Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumer keystrokes).

Phishing (sometimes called carding or brand spoofing) uses e-mail messages that purport to come from legitimate businesses that one might have dealings with, such as: I) banks; ii) online organizations; iii) Internet service providers; iv) online retailers; and, v) insurance agencies. The messages may look quite authentic and may feature corporate logos and formats like the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes or security concerns of the account.

“Smashing”

Like Phishing, Smashing uses cell phone text messages to deliver the "bait" to get consumers to divulge their personal information. The "hook" (the method used to capture your information) in the text message may be a Web site Uniform Resource Locator (URL), however it has become more common to see a telephone number that connects to automated voice response system.

The Smashing message usually contains something that wants your "immediate attention". Some examples include "We're confirming you've signed up for our dating service. You will be charged $2/day unless you cancel your order on this URL: www.?????.com.”; or “(Name of popular bank) is confirming that you have purchased a $1500 computer from (name of popular computer company). Visit www.?????.com if you did not make this online purchase."; or, "(Name of a financial institution): Your account has been suspended. Call ###. ###. #### immediately to reactivate."

The hook is a legitimate looking Web site that asks you to confirm or enter your personal financial information, such as your credit/debit card number, CVV code (on the back of your credit card), your ATM card PIN, Social Security Number, e-mail address, or other personal information. If the hook is a telephone number, it normally directs the person to a legitimate sounding automated voice response system, like the voice response systems used by many financial institutions, which will ask for the same personal information.

This is an example of a Smashing message in current circulation: "Notice - this is an automated message from (a local financial institution), your ATM card has been suspended. To reactivate, please call immediately at 866-###-####.”

In many cases, the Smashing message will show that it came from "5000" instead of displaying an actual phone number or from a company domain. This usually indicates the message was sent via e-mail to the cell phone, and not sent from another cell phone. The information is then used to duplicate ATM/credit/debit cards. There are documented cases where information entered on a fraudulent Web site (used in a Phishing, Smashing, or Vishing attack was used to create a credit or debit card that was used halfway around the world.

“Vishing”
Also called "VoIP phishing," it is the voice counterpart to Phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's credit card number. The initial bait can also be a telephone call with a recording that instructs the user to telephone a toll-free number.

Whether Phishing or Vishing, because people are used to entering credit card numbers over the telephone, this technique may be effective. Voice over IP (VoIP) is used for Vishing because caller identifications can be spoofed, and the entire operation can be brought up and taken down in a short time, compared to a real telephone line.

Identity Theft

How You Can Protect Yourself?

Internet Pirates are trying to steal YOUR personal financial information. Want the good news?

YOU have the power to stop them. There is a new type of Internet piracy called Phishing (see above definition). It’s pronounced "fishing" and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security Numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards. In the worst case, you could find yourself a victim of identity theft. With the

sensitive information obtained from a successful Phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in YOUR name. They can do damage to your financial history and personal reputation that can take years to unravel. But if you understand how Phishing works and how to protect yourself, you can help stop this crime. Please refer to the Phishing section above.

Protecting Yourself

You can protect yourself by never providing your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information. If you believe the contact may be legitimate, contact the financial institution yourself. You can find telephone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself. Never provide your password over the telephone or in response to an unsolicited Internet request. A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.

Also, review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity. If you fall victim to a thief, contact your financial institution immediately and alert them of the situation. If you have disclosed sensitive information in a Phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. The contact information for each credit bureau's fraud division is:

- Equifax 800-525-6285 [P.O. Box 740250 Atlanta, GA 30374]
- Experian 888-397-3742 [P.O. Box 1017 Allen, TX 75013]
- TransUnion 800-680-7289 [P.O. Box 6790 Fullerton, CA92634]

And report all suspicious contacts to the Federal Trade Commission by calling (877)-IDTHEFT (1-877-438-4338) or through the Internet at https://www.ftccomplaintassistant.gov.

In summary, never provide personal financial information, including your Social Security Number, account numbers, or passwords, over the telephone or the Internet if you did not initiate the contact. Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer. Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information. If you believe the contact is legitimate, go to the company's Web site by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail. If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.

What to do if you believe your New Century Bank account has been compromised: New Century Bank does not contact customers to request or verify security information about login id's, passwords, PIN's or other security measures in place to protect your account. However, when you contact New Century Bank, our employees may ask for specific information to verify your identity to ensure your privacy and protection. If you feel your New Century Bank account has been compromised, contact us at (785) 527-2772.

It is our goal to keep consumers informed and educated in taking the right precautions to avoid becoming a victim of identity theft and account fraud. If you have any questions, feel free to contact your local office, Monday thru Friday 8:00 am until 5:00 pm Central Standard Time. We are closed Saturday and Sunday.

For more information on Identity Theft and other types of account fraud, please visit the following websites:

- United States Postal Inspection Service: https://postalinspectors.uspis.gov/
- Federal Trade Commission: Visit http://www.ftc.gov/bcp/edu/microsites/idtheft/
- United States Secret Service: Visit http://www.secretservice.gov/
- United States Department of Justice: Visit http://www.usdoj.gov/
- Federal Deposit Insurance Corporation: Visit http://www.fdic.gov/

Elder Abuse

Elder abuse is one of the most disturbing and rapidly growing areas of crime in our society. Abuse comes in many forms: physical, emotional or financial exploitation. The elderly is especially vulnerable to financial abuse that can be devastating and leave them without the finances to provide for their needs. Under federal and state law, residents in skilled nursing facilities are guaranteed certain rights and protections.

Examples of financial elder abuse include embezzlement of money or any other property, telemarketing fraud, identity theft, predatory lending and home improvement and estate planning scams.

We should all be doing our part to ensure that the elderly is given the opportunity to live with security and dignity, whether they live independently, with family, in an assisted-living setting or a long-term care facility.

For more information visit the California Department for Aging and Disability Services visit:
https://www.kdads.ks.gov/

Best Practices on Spyware Prevention and Detection

The Internet has become a popular method for both conducting business and managing finances through online banking relationships. While most financial institutions and some individuals have taken steps to protect their computers, many firewall and anti-virus software packages do not protect computers from one of the latest threats, Spyware, which is a form of software that collects personal and confidential information about a person or organization without their proper knowledge or informed consent and reports it to a third party.

Spyware Infection:

Spyware is usually installed without a user's knowledge or permission. However, users may intentionally install spyware without understanding the full ramifications of their actions. A user may be required to accept an End User Licensing Agreement, which often does not clearly inform the user about the extent or way information is collected. In such cases, the software is installed without the user's informed consent. Spyware can be installed through the following methods:

I. downloaded with other Internet downloads in a practice called bundling (in these cases the licensing agreements may be included in one pop-up window that unless read carefully may leave the user unaware of bundled spyware);
II. directly downloaded by users who were persuaded that the technology offers a benefit (some spyware claims to offer increased productivity, virus scanning capabilities or other benefits);
III. installed through an Internet browsing technique called drive-by downloads (this technique involves spyware being installed when a user simply visits a Web site and the user may be

prompted to accept the download believing it is necessary in order to view the Web page); or, iv) automatically downloaded when users open or view unsolicited e- mail messages.

Behaviors Associated with Spyware:

Spyware can be difficult to detect and remove because it does not always appear as a running program in the Windows Task Manager; therefore, the user may be unaware that his or her computer is infected. Spyware may not include a removal option in the Windows Add/Remove Programs function. When such an option is present, the removal process may not eliminate all components, or it may redirect the user to an Internet site to complete the removal. This often results in new or additional infection rather than removal. In addition, some spyware includes a feature to re-install itself when any portion is deleted. Spyware may cause a further infestation by installing other spyware programs onto users' computers.

Risks Associated with Spyware:

Spyware increases the risk by exploiting security vulnerabilities or settings, changing the computer configuration to relax security settings, or allowing a channel into the computer system by circumventing the firewall. The result is that attackers can eavesdrop and intercept sensitive communications by monitoring keystrokes, e-mail and Internet communications. This monitoring may lead to the compromise of sensitive information, including user names and passwords. Spyware may provide attackers the ability to control corporate computers to send unsolicited junk e-mail (SPAM) or malicious software (Malware), or to perform denial of service (DoS) attacks against other organizations. Spyware may drain system resources and productivity and consume system resources, even when the user is not browsing the Internet, such as when adware results in voluminous unwanted pop-up advertisements. Spyware may even compromise the ability to conduct business by disrupting Internet connections as a result of the improper removal of spyware. Spyware may increase the incidence of SPAM to e-mail accounts. And Spyware may compromise confidentiality. Certain types of spyware route all Internet communications through their own servers, often without the user's knowledge. This allows a third party to read sensitive Internet communications even when Secure Socket Layer (SSL) or other encryption protocols are used. Other forms of spyware install an application on the user's computer that monitors and records all Internet communications and sends the report back to the originator. Identity thieves may then impersonate the customer using the user names and passwords collected.

New Century Bank educates clients about the risks associated with spyware and encourages clients to implement steps to prevent and detect spyware on their own computers. In addition, the Bank advises clients of the risks of using public computers to connect to online banking websites. And by implementing multi-factor authentication methods, the Bank limits the ability of identity thieves to compromise client accounts, even when a thief has a client's identification, user name, password or even account number.

New Century Bank recommends to our clients that they may prevent and detect spyware by:

I. installing and periodically updating anti-spyware, virus protection and firewall software;
II. adjusting browser settings to prompt the user whenever a Web site tries to install a new program or Active-X control (an Active X control is a set of instructions that will automatically run on a computer when downloaded bythe browser);
III. carefully reading all End User Licensing Agreements and avoiding downloading software when licensing agreements are difficult to understand; iv) maintaining patches to operating systems and browsers; and, v) not opening e-mail from untrustworthy sources.

ATM Safety

Your safety is important to us and we would like to encourage you to keep the following tips in mind when using your card at an ATM:

- Be aware of your surroundings before conducting an ATM transaction. If you see someone or something suspicious, leave and come back later.
- When using a walk-up ATM, park as close as possible and check for suspicious persons or circumstances before leaving the safety of your car.
- Do not leave your car running or the keys in the ignition while at the ATM. As you return to your vehicle, have your car keys ready and check around you and under your vehicle.
- If possible, have someone accompany you to the ATM and have your ATM card ready before you approach the machine.
- Use an ATM located in a highly trafficked area for additional security.
- Check the card reader to ensure it has not beentampered with.
- Use your body and hands to shield the screen or keypad when entering your PIN.
- Do not count your money while at the ATM. Put your money, receipt and card away immediately and do not linger at the ATM.
- Do not discard receipts for ATM transactions. Verify receipts against your monthly bank statement and report any discrepancies immediately.
- If you are followed using an ATM, head to a place where activity, people and security can be found. Call the police if necessary.
- If you are followed using an ATM, seek a place where people, activity and security can be found. If necessary, call the police.
- Do not count your money while at the ATM. Put your money, receipt and card away quickly. Always take your ATM receipt, which is stamped with your transaction.
- When using a walk-up ATM, park as close as you can to the machine. Before leaving the safety of your car, check for suspicious persons or circumstances. Have your ATM card ready before you approach the machine?
- Do not leave your car running or the keys in the ignition as you walk up to an ATM. As you return after your transaction, have your car keys ready and check around and under your vehicle.

Other things to keep in mind:

- Treat your ATM card like cash and ALWAYS keep it in a safe place.
- Keep your Personal Identification Number (PIN) secret. Never write your PIN on our card, tell your code to anyone or allow anyone to enter your PIN.
- Do not give out any information about your ATM card over the telephone. The Bank will never ask you for your PIN.