PRIVACY NOTICE

Rev. March 2014

FACTS WHAT DOES CITIZENS BUSINESS BANK DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: • Social Security number and Investment Experience • Account Balance and Payment History • Transaction History and Credit History When you are no longer our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Citizens Business Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Citizens Business Bank Share?	Can you limit this sharing?
For our everyday business purposes? such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes? to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates? everyday business purposes? information about your transactions and experiences	No	We don't share
For our affiliates? everyday business purposes? information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions?	**Call (888) 228-2265 or go to www.cbbank.com**

What we do	
How does Citizens Business Bank protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does Citizens Business Bank collect my personal information?	We collect your personal information, for example, when you • open an account or deposit money • pay your bills or apply for a loan • use your credit or debit card We also collect your personal information from others, such as credit bureaus, affiliates, or other companies
Why can?t I limit all sharing?	Federal law gives you the right to limit only • sharing for affiliates' everyday business purposes?information about your creditworthiness • affiliates from using your information to market to you • sharing for nonaffiliates to market to you

	State laws and individual companies may give you additional rights to limit sharing.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. • *Citizens Business Bank does not share with our affiliate.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. • *Citizens Business Bank does not share with nonaffiliates so they can market to you.*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. • *Citizens Business Bank doesn't jointly market.*

ONLINE PRIVACY

Last updated: March 17, 2014

Your California Privacy Rights

Under California law, we will not share information we collect about you with companies outside of Citizens Business Bank, unless the law allows. For example, we may share information without your consent, to service your accounts.

How Personal Information is Shared

Please see the Citizens Business Bank Privacy Notice for information on how Personal Information may be shared. Click Here

Personal Information We Collect Online

Personal information means personally identifiable information such as information you provide through Online Banking including name, postal or email addresses, telephone numbers, date of birth, social security number or account numbers. You have the ability to update your e-mail address, security questions and passwords that are stored in your Online Banking profile. You may do so by logging on to your Online Banking account, selecting Options from the main menu bar and following the prompts for updating this information.

Keeping your account information accurate and up to date is very important. Please use the Contact Us option on our website, or call or write us at the telephone number or appropriate address that is located on your account statement, on our website, or on other account materials, to update your information and/or to notify us of the change you made to your e-mail address through Online Banking. You can also notify us by visiting a Bank Representative at any of our locations.

Visitors to Our Web Site

As a visitor to our web site, you remain anonymous, unless you register for Online Banking or visit our “Contact Us” page and disclose your identity to us. Although we do not collect personal information that identifies people who simply visit our site, we may collect certain limited information about our visitors, such as their IP address (a numeric address assigned automatically to computers and mobile devices when they access the internet).

Children's Online Privacy Protection Act

Our web site is directed to a general audience. We do not knowingly solicit, collect or provide links to other web sites that may solicit or collect personal information from children under age 13.

Children's Internet Protection Act

Updates to the Online Privacy Notice

This Online Privacy Notice is subject to change. Please review periodically. If we make changes to the Online Privacy Notice, we will revise the “Last Update” date at the top of this Notice. Any changes to this Notice will become effective when we post the revised Notice on our site. Your use of our site following these changes means that you accept the revised Notice.

SECURITY INFORMATION

Security Statement

This Internet Banking System brings together a combination of industry-approved security technologies to protect data for the bank and for you, our customer. It features password-controlled system entry, a VeriSign-issued Digital ID for the bank's server, Secure Sockets Layer (SSL) protocol for data encryption, and a firewall to regulate the inflow and outflow of server traffic.

Secure Access and Verifying User Authenticity

To begin a session with the bank's server the user must enter a Log-in ID and a password. Upon successful login, the Digital ID from VeriSign, the experts in digital identification certificates, authenticates the user's identity and establishes a secure session with that visitor.

Secure Data Transfer

Once the server session is established, the user and the server are in a secured environment. Because the server has been certified as a 128-bit secure server by VeriSign, data traveling between the user and the server is encrypted with Secure Sockets Layer (SSL) protocol. With SSL, data that travels between the bank and customer is encrypted and can only be decrypted with the public and private key pair. In short, the bank's server issues a public key to the end user's browser and creates a temporary private key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a new end user makes a server session.

Firewall

Requests must filter through a firewall before they are permitted to reach the server. A firewall, is a device which blocks and directs traffic coming to and from the server passing only acceptable data requests, such as retrieving web pages or sending customer requests to the bank.

Cookies

We will occasionally use a "cookie" for the purpose of providing improved service. A cookie is a small bit of information given to your browser by a Web site, which can later be retrieved. A cookie is a way for a Web site to recognize whether or not you have visited the site before. The cookie can only be read by the Web site that "set" the cookie. We use cookies for administrative purposes, such as online banking session management, or where you are able to customize the information you see. The use of cookies makes your online experience easier and more personal. Most cookies last only through a single session, or visit. They do not read your hard drive or contain any information that you have not already explicitly revealed. None will contain information that will enable anyone to contact you via telephone or e-mail. Your Web browser can be set to inform you when cookies are set or to prevent them from being set. However, if you elect to prevent cookies from being set, some Web banking functions may not work properly.

Cache Storage of Web Site Information

Internet browser software typically stores - or "caches" - information from the Web site being visited on the hard drive of the browsing computer for a period of time. This means that information viewed or input during a visit to a Web site can usually be viewed again merely by hitting the "Back" button in the browser application. (Some Web sites issue a "no-cache" command to browsers to prevent temporary "cache" storage from occurring.) To provide optimum performance to those who visit our Web site, we do not send a no-cache command to browsers.

To prevent others from viewing confidential information cached on the computer's hard drive during your visit to our Web site, you must clear your cache before leaving your computer accessible to another person.

Email Security

Internet e-mail is not secure. When sending an e-mail to us, do not provide sensitive or confidential information (for example, your account number). You may contact our ServiceLine at 1(888) 222-5432 (toll-free) during business hours, Monday through Friday between 8:00 a.m. to 6:00 p.m. or visit any of our offices if you need assistance.

Linking to Other Sites

We may provide links to other Web sites that are not controlled by Citizens Business Bank. If you choose to link to Web sites that are not controlled by Citizens Business Bank, we are not responsible for the privacy or security of these sites. You are encouraged to review the Web site's privacy policy before providing any personal information. In addition, Citizens Business Bank does not guarantee the products, information or recommendations provided by these sites.

Aggregation Sites

Aggregation sites are Internet sites that allow you to consolidate account information from several sources on one site. To do this, an aggregation provider may request access to your personal financial information. You should ensure that the aggregator company has adequate policies to protect the privacy and security of any information you provide or to which they are gaining access, and that you trust the aggregator company.

If you provide information about your Citizens Business Bank accounts to an aggregator company, we will consider that you have authorized all transactions initiated by an aggregation site using access information you provide, whether or not you were aware of a specific transaction. If you decide to revoke the authority you have given an aggregator company, it is important that you notify us to ensure that you may continue to access your account.

Risk of Unauthorized Access Awareness and Mitigation

The Bank offers certain clients online banking services that provide the ability to access account information and transfer funds electronically. One of the risks associated with online banking is unauthorized access, which could result in the unintentional exposure of sensitive account information and the unauthorized origination of electronic transactions. Unauthorized access could lead to significant losses.

One commonly used method for cybercriminals to gain access to your computer – and possibly your online banking and electronic funds transfer services – is through the download of malicious software (malware) to your computer system. An individual clicking on a compromised website, link or email attachment can inadvertently trigger the download of malware onto the victim's computer. Malware may perform any number of sinister attacks, including quietly capturing every keystroke a victim makes on his or her computer keyboard, which is then automatically transmitted to the cybercriminal who originated the attack. If any captured keystrokes include the victim's online banking credentials, the cybercriminal may thereby gain access to the victim's online banking services, which could allow the cybercriminal to view sensitive account information and create unauthorized funds transfer or other electronic transactions.

The risk of fraud can be mitigated by, among other things, your establishing a sound Internet use policy and taking steps to prevent malicious software from being loaded on your computer, which may include but is not limited to (i) employing firewalls, (ii) daily updates to your antivirus/anti-malware software, (iii) restricting individual access to computers used for online banking, (iv) restricting Internet access and websites available to computers used for online banking, (v) locking down and password-protecting wireless networks, (vi) and dedicating a computer for only online banking purposes. All of these strategies should be implemented when utilizing online banking services, particularly when originating funds transfer or other electronic transactions. In addition, you should review on a daily basis all your account balances and detailed transactions and report any suspicious activity to the Bank immediately.

We recommend that you implement as many of the above recommended procedures and tools as possible in order for you to reduce your risk of being victimized by fraud. It is important to note that while these practices can significantly mitigate the risk of unauthorized access, there are no foolproof methods to completely eliminate all the risks and all the exposure to loss.

Also, please consider the following:

Keep in mind that OUR BANK WILL NEVER ASK YOU FOR YOUR CONFIDENTIAL CREDENTIALS, ACCESS CODES OR OTHER SECURITY

PROCEDURES. If you receive an e-mail that looks like it came from our Bank, but asks you for this type of information, you should not respond to the email and you should immediately report the incident to the Bank's Client Support team at (888) 228-2265. The sender is not our Bank, and is likely a criminal.

You should conduct a periodic risk assessment of your environment as it relates to Internet access, online banking, and funds transfers. Most clients find the potential risk exposure high enough to justify the cost of using an outside expert in this field to assist them. The risk assessment should assess your overall Internet exposure, online banking exposure and existing mitigation systems (such as procedural, technical and administrative safeguards that you use). We ask that, if not already employed, you again consider the alternatives we have previously offered that can help reduce the risks of fraud and losses associated with Internet access, online banking and electronic funds transfers.

Again, no system or set of systems is fool-proof, but we do know that the risks of fraud can be significantly reduced when clients use the risk mitigation strategies and tools referenced above. Please feel free to contact Client Support at (888) 228-2265 and a subject matter expert would be happy to explain these strategies again and in more detail.

If you choose not to implement the risk mitigation strategies and tools referenced above, please do so only after considering the substantial and multiple risks of fraud to which your business is exposed without these mitigants. Your risk of unauthorized funds transfer activity can be significantly higher if you choose to forgo the risk mitigation strategies and tools offered by the Bank or outside experts as mentioned above.