MISSION VALLEY BANK

DIGITAL PRIVACY AND COOKIES POLICY

Introduction and Scope of Policy

This Digital Privacy and Cookies Policy ("Policy") applies to your interaction with Mission Valley Bank ("we," "us," or "our"), via this website or any mobile app that we own or control, including the Business Mobile app and the Small Business & Personal Mobile Banking app, both of which are available through Apple and Google (collectively referred to as "Site"). Other digital policies or privacy policies may also apply. This Policy explains certain data use and data practices, and our online ads, such as banner ads on third party sites.

Agreement to Policy

By using this or any Site, you consent to this Policy, including your consent to our use and disclosure of information about you in the manner described in this Policy.

Children's Privacy

We do not provide services or sell products to children. If you are below the age of 18, you may use our website only with the permission and active involvement of a parent or legal guardian. If you are a minor, please do not provide us or other website visitors with any personal information. We do not knowingly collect personal information via our web pages from individuals under the age of 13 without obtaining verifiable consent from their parents. We ask that individuals under the age of 13 never provide personal information through the Site.

For more information about the Children's Online Privacy Protection Act (COPPA), visit the FTC website. (www.ftc.gov)

Gathering, Using, and Sharing Information

Types of Information

You may interact with Mission Valley Bank in a variety of ways online, including through a mobile device. We may also offer the ability to enroll, register, or access your accounts online. We may offer apps that permit browsing and do not require registration. Information that we may collect about you through online interaction includes information that you input, such as your name, address, email address, other contact information; data resulting from your activity, such as transaction information; and location information. We may also gather additional information, such as the type of device and browser you are using, the IP address of your device, information about your device's operating system, and additional information associated with your device. We may also gather information collected through cookies, tags, and other technologies, as described further below.

About "Cookies" and Ad Choices on Third Party Sites

Cookies are pieces of data stored on your device. Browser cookies are assigned by a web server to the browser on your device. When you return to a site you have visited before, your browser gives this data back to the server. Mobile app may also use cookies.

At present, we do not do send out web-based advertising. Any outbound email from us regarding news, events, or seminars are sent to those who opt in only and all such communications will include opt-out options within the message. Eventually, we may use cookies and information gathered through your use of Sites to make your experience with Mission Valley Bank more personalized based on the products, services, or other interaction you have with us and other sites. Information gathered through use of cookies may be used to make offers to you via online ads, email, U.S. mail, or telephone, subject to the privacy preferences you have on file with Mission Valley Bank. (Privacy preferences for employer-sponsor retirement accounts will always default to no marketing, solicitation, or sharing for marketing purposes without specific consent.)

Information that we collect about you from one particular browser or device may be used to provide advertising or collect information on another browser or device. It may also be transferred to a third party for advertising or information collection on behalf of Mission Valley Bank. Please note that your choice to opt out on a particular browser or device will apply only to the collection and use of information from that particular browser or device. Opting out on a particular device will not opt you out of information collection on other devices, nor will it limit cross device sharing on those other devices. 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.

Other parties may collect information about your web browsing behavior when you use our Site. But these parties are generally limited to service providers who may only use any information collected to provide services and marketing for us and not to provide services or advertising for any other party. We may also use cookies for purposes such as maintaining continuity during an online session; gathering data about the use of our site; monitoring online promotions; and anti-fraud and information security purposes.

Accepting Cookies

You may be able to set your browser to reject browser cookies. However, if you choose to reject cookies, your ability to access your accounts with Mission Valley Bank apps may be limited. Therefore, if you set your browser options to disallow cookies, you may limit the functionality we can provide when you visit our Site. The latest versions of internet browsers provide cookie management tools, such as the ability to delete or reject cookies. We recommend that you refer to information supplied by browser providers for more specific information, including how to use these tools.

Additional cookies

Cookies is a term also used to describe other locally stored objects, such as cookies stored in an Adobe folder on your device. These cookies will not be deleted when you clear cookies from your browser. We may use this technology for purposes such as information security and fraud prevention. We do not use this technology for online behavioral advertising purposes. Please refer to information provided by Adobe for information on how to disable and control Flash objects. If you choose those options, you may limit the functionality we can provide when you visit our Site.

Additional Technologies

We may someday use additional technologies such as pixel tags, web beacons, and clear GIFs, and may permit our third-party service providers to use these technologies. These technologies are used for measuring the effectiveness of our advertisements or other communications, determining viewing and response rates, and determining which offers to present to you on our own or on third-party sites.

Using Information

We may also use the information described above for purposes such as: servicing; communicating with you; improving our Site, products, or services; legal compliance; risk control; information security; anti-fraud purposes; marketing or personalizing the presentation of our products and services to you; tracking website usage, such as number of hits, pages visited, and the length of user sessions in order to evaluate the usefulness of our sites; and using read-receipt notifications in our email communications, but always only as allowed by law.

Sharing Information

We may share information with service providers with whom we work, such as data processors and companies that help us market products and services to you. When permitted or required by law, we may share information with additional third parties for purposes including response to legal process. As applicable, please see the additional privacy policies referenced above, such as the Mission Valley Bank U.S. Consumer Privacy Notice, for more information on how we may share information with affiliates and third parties. (https://www.missionvalleybank.com/pdf/Privacy-Notice.pdf)

Any updates to the Policy become effective when we post the updates on the Site. Your use of the Site following the update to the Policy means that you accept the updated Policy.

Risk of Unauthorized Access Awareness and Mitigation

We offer 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 transfers or other electronic transactions.

The risk of fraud can be mitigated if you establish a sound internet use policy and take 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, and (vi) 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 us immediately.

We recommend that you implement as many of the above procedures and tools as possible in order 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:

WE 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 us, but asks you for this type of information, you should not respond to the email and you should immediately report the incident to us. The sender is not us, 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 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).

Again, no system or set of systems is foolproof, but the risks of fraud can be significantly reduced by using the risk mitigation strategies and tools referenced above.

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 you will be exposed. Your risk of unauthorized funds transfer activity can be significantly higher if you choose to forgo these risk mitigation strategies.

Questions

If you have questions or concerns you may address them to us by email or at the following address:
Mission Valley Bank
9116 Sunland Boulevard
Sun Valley, CA 91352
USA

This Digital Privacy and Cookies Policy was last updated on December 5, 2018.

09/2019