CBB California Business Bank

This document outlines best practices for fraud prevention for Digital One Business users.

User ID and Password Guidelines

- Create a "strong" password with at least eight characters that includes a combination of mixed case letters, numbers, and special characters.

- Change your password frequently.

- Never share user name and password information with third-party providers.

- Avoid using an automatic login feature that saves user names and passwords.

General Guidelines

- Do not use public or other unsecured computers for logging into Digital One Business.

- Check the last login date/time every time you log in.

- If the system does not recognize your computer or location, you will be asked to provide additional information to log into Digital One Business. This may include Out-of-Band Authentication via phone or SMS text message.

- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.

- View the available transfer history by viewing account activity information.

- Whenever possible, use Bill Pay instead of checks to limit account number exposure and to obtain better electronic record keeping.

- Take advantage of and regularly view system alerts; examples include:

- Balance alerts

- Password change alerts

- Transfer alerts

- ACH alerts

- Wire alerts

- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.

- Use the historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.

- Never leave a computer unattended while using Digital One Business.

- Never conduct banking transactions while multiple browsers are open on your computer.

Administrative Users

- Prohibit the use of "shared" user names and passwords for Digital One Business.

- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.

- Dedicate and limit the number of computers used to complete online banking transactions. Do not allow internet browsing or email exchange and ensure these computers are equipped with latest versions and patches of both antivirus and anti-spyware software.

- Delete online user IDs as part of the exit procedure when employees leave your company.

- Use multiple approvals for monetary transactions and require separate entry and approval users.

- Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers, and account transfers.

- ACH (Automated Clearing House) Batches

- Use pre-notification transactions to verify that account numbers within your ACH payments are correct.

- Use limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

- Review historical and audit reports regularly to confirm transaction activity.

- Use available alerts for ACH activity.

Wire Transfer

- Use limits provided for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

- Review historical and audit reports regularly to confirm transaction activity.

- Use available alerts for wire transfer activity.

Account Transfer

- Use limits provided for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

- Review historical and audit reports regularly to confirm transaction activity.

- Use available alerts for external transfer activity.

Tips to Protect Online Payments and Account Data

- Take advantage of transaction limits. Establish limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

- When you have completed a transaction, ensure you log off to close the connection with the financial institution's computer.

- Use separate accounts for electronic and paper transactions to simplify monitoring and tracking any discrepancies.

- Reconcile by carefully monitoring account activity and reviewing all transactions initiated by your company on a daily basis.

Tips to Avoid Phishing, Spyware, and Malware

- Do not open email from unknown sources. Be suspicious of emails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as user names, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious emails could expose your system to malicious code that could hijack your computer.

- Never respond to a suspicious email or click on any hyperlink embedded in a suspicious email. Call the purported source if you are unsure of who sent an email.

- If an email claiming to be from your financial institution seems suspicious, check with your financial institution.

- Install antivirus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.

- Update all of your computers regularly with the latest versions and patches of both antivirus and anti-spyware software.

- Ensure computers are patched regularly, particularly operating systems, browsers, and key applications.

- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.

- Check your settings and select, at least, a medium level of security for your browsers.

- Clear the browser cache before starting any Digital One Business session to eliminate copies of webpages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.

- Be advised that you will never be presented with a maintenance page after entering login credentials. Legitimate maintenance pages are displayed when first reaching the URL and before entering login credentials.

- Digital One Business does not use pop-up windows to display login messages or errors. They are displayed directly on the login screen.

- Digital One Business never displays pop-up messages indicating that you cannot use your current browser.

- Digital One Business error messages never include an amount of time to wait before trying to login again.

- Be advised that repeatedly being asked to enter your password/token code are signs of potentially harmful activity.

Tips for Wireless Network Management

- Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router/access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.

- Disable remote administration of the wireless network hardware (router/access point).

- If possible, disable broadcasting the network SSID.

- If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.

- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.