WestStar

Don't Fall Victim To Fraud! Here Are Some Tips To Protect Your Business.

WestStar considers your privacy and security our top priority and we want to provide you with the following industry best practices to help reduce the risks associated with corporate account takeover fraud.

The following industry best practices will not provide a guarantee against fraud, but will greatly lower the exposure to many of the common threats and risks that are often seen with fraud:

- Provide security awareness training to your employees, particularly those with access to your financial information. **Your employees are your first line of defense.** Visit our **Cybersecurity Center (https://www.weststarbank.com/cybersecurity-center)** for more information on how to protect your personal or financial information.
- Computer(s) used for Cash Manager should be strictly used only for Cash Manager services and are not used for internet or email access.
- Computer(s) used for Cash Manager should have anti-virus, spyware, and malware protection that is updated regularly with scheduled scans performed periodically. Additionally, operating systems and web-browsers should also be updated with the latest updates and have a firewall. Please note that for WestStar's Cash Manager clients, WestStar provides Trusteer Rapport software (free of service) that can help protect against financial malware and phishing attacks.
- Use of separate devices to originate and transmit wire and/or ACH transactions.
- Perform dual controls for submitting and approving transactions.
- Personal and confidential information, such as physical addresses, phone numbers, dates of birth, city of birth, mother's maiden name, or Social Security Numbers, should not be posted on social media websites or comments sections.
- Use unique passwords and do not include words of identifiable information, such as an address, birthday, birthplace, name of a family member, or pet. Additionally, passwords should be set at 8 characters or more, and include three of the following: a number, a special character, a lower case, and an upper case. **NEVER disclose your online banking or cash manager credentials.**
- Emails containing financial account information or other information that could provide access to banking accounts should not be sent over unsecured email. This includes account numbers, bank names, login IDs, passwords, and other confidential information. [To send confidential information to WestStar, the use of the Secure Messaging Portal is recommended. **https://www.weststarbank.com/secure-messaging-portal**]
- Periodically review and deactivate or remove cash manager access rights from employees that no longer require access (e.g., inactive, transferred, or terminated employees). For assistance with access to our Cash Manager Service, our Treasury Management department is ready to help.
- Links and attachments in emails should always be treated with suspicion. Be wary of unsolicited links and attachments, even from known contacts as they can also potentially be compromised. Always verify unexpected emails with the source using other means (e.g. follow-up with a phone call).
- Always shred documents containing confidential information; this information typically is the account number, name, address, bank, or other identifying data that could be used to allow unauthorized access.
- Practice ongoing account monitoring, reconciliation and report any discrepancies or suspicious activity immediately. Subscribing to E-statements is also encouraged to reduce the risk of mail theft.
- Enable transaction and balance alerts for debit cards and/or deposit accounts that alert when transactions are completed or if the balance changes significantly.
- Adopt advanced security measures and response by working with IT/Security consultants or dedicated staff.
- Utilize resources provided by trade organizations and agencies that specialize in helping small businesses.

We encourage all of our Cash Manager clients to take the above steps to better protect themselves against corporate account takeover fraud. A secure banking environment is a partnership between you and your bank, and one we take very seriously. The security of your information is more important than ever.