



Security Recommendations

To protect your system from security breaches, you should adopt internal controls and guidelines that include:

- a) **Implement dual custody.** Adopt dual authorization and/or transaction-based authentication procedures for financial transfers.
- b) **Protect your machines.** Place limits and controls on who has access to your computer systems.
- c) **Protect your Password.** Protect and frequently change your Password and never share your user credentials.
- d) **Update antivirus software and patch your machines.** Ensure that your company's firewalls, servers and client machines are updated with all vendor-recommended patches and that antivirus and anti-spy ware software is installed and updated. Use commercially reasonable and up-to-date firewalls and intrusion prevention technologies.
- e) **Be cautious.** Use caution if you receive an e-mail or text message expressing an urgent need for you to update your information, activate an account, and verify your identity by calling a phone number or submitting information on a Web site. Also practice caution with e-mail attachments and downloadable files. Know that Fremont Bank does not ask for confidential information through e-mail and that e-mail attachments and downloadable files from any external source could be harmful to your computer.
- f) **Educate your employees.** Educate your employees about online fraud and train them never to give out their online banking access credentials. Their passwords, PINs, and token codes open the door to your accounts. Remind employees to stay on their guard. Allow online banking services to be accessed only from a secure location on your premises.
- g) **Limit your exposure.** Implement procedures to avoid infection by malicious software, such as: controlling what websites are visited by your computers; controlling the connection of other devices (e.g., flash drives) to your computers; controlling what documents, e-mail attachments, programs and other files are opened or installed on your computers; and limiting which of your computers are used for online banking. Prohibit your authorized users from leaving a computer unattended while connected to our system or from communicating or accessing sensitive information from insecure locations (e.g., terminals at Internet cafes and airports).
- h) **Use stand-alone PCs for your online banking.** If possible, use stand-alone PCs for your online banking transactions that are not enabled for e-mail or general web browsing. If using stand-alone PCs is not possible, do not conduct non-essential e-mail or Web browsing, specifically to social media sites, from your PC.
- i) **Protect your network.** Identify trusted Web sites for your business and block access to any site/Web address that would not be relevant to your employees' business needs.
- j) **Let us help you.** Use fraud protection services such as Positive Pay for checks issued and ACH Monitoring Service, including debit and credit blocks for unauthorized ACH entries



to your account. Also, use payment templates to prevent unauthorized modifications, and ensure that your payment limits reflect your typical transaction amounts.

- k) **Keep up to date.** We have attached a recent FS-ISAC publication explaining threats and security countermeasures. Regularly check antifraud sites for new threats and best security practices.

<http://www.ftc.gov/bcp/edu/microsites/infosecurity/>

Vigilance and regular monitoring of account activity is thoroughly recommended. Audit and verify all transactions on a regular basis, and regularly reconcile your accounts.

- l) **Monitor online accounts daily.** Actively monitor your online accounts to detect suspicious activities. Immediately contact your customer service group if you notice anything out of the ordinary.

This is not a complete listing of the internal security controls that you may need. You are responsible for determining and implementing whatever controls are necessary to prevent security breaches and internal security losses. We do not warrant that any or all of the above recommendations will prevent a security breach.