svb
Silicon Valley Bank

Consumer best practices in fraud prevention

Follow these tips to help mitigate your fraud risk

You play a critical role in the prevention and detection of fraud on your financial accounts. Below are some risks you need to be aware of, and steps you can take to help protect yourself from fraud.

Identity theft

- Avoid sending personal or financial information via phone or internet unless you initiate the conversation
- Destroy documents (like bank or billing statements and receipts) that include personal or financial data
- Immediately notify SVB in advance of travel events, including the location and dates of travel
- Request free credit reports annually and review them for inaccuracies. For consumer information, check https://www.consumer.ftc.gov/articles/0155-free-credit-reports
- Reconcile your banking transactions on a daily basis
- Don't give your personal or financial information to anyone who contacts you claiming to be from SVB. We will never request this information when we contact you
- Keep your SVB online banking contact information up to date, including email addresses and phone numbers
- Be cautious when entering personal information on websites such as social networks, job sites
- Check your email and browser privacy settings to adjust relevant privacy controls on social media sites
- Don't use personal information in your user name or email address

Phishing scams

Watch out for emails, phone calls and texts that

- Require you to give your personal or account information
- Pressure you or threaten to close or suspend your account if you don't take immediate action
- Contain grammatical errors or awkward writing
- Inform you of an unauthorized charge and ask you for personal or account information
- Include an offer that sounds too good to be true such as a tax scam. Visit https://www.irs.gov/compliance/criminal-investigation/irs-wants-you-to-know-about-schemes-scams-and-cons for more information on how to avoid tax fraud

Card fraud protection

- Don't provide your card number over the phone or online unless the company is known to be reputable and you initiated the transaction
- Ensure websites are secure (e.g., starts with https:// or includes a lock symbol in your browser bar) when entering personal or financial information online
- Don't lend your card to anyone
- Notify SVB immediately if your card is lost or stolen, if you don't recognize a transaction, or if you suspect unusual activity on your card
- Limit the number of cards you carry in your wallet
- Do not carry your Social Security card
- Create a secure PIN that is not easily guessed
- Keep your PIN secure, not on your phone or your card
- Be wary of ATMs that appear altered or crooked, there could be a skimming device attached
- Shield the keypad while entering your PIN

Cyber security and other best practices

- Use a dedicated and actively managed firewall
- Install and update antivirus and security software
- Download IBM Security Trusteer Rapport® by visiting https://www.svb.com/fraud-trusteer/
- Use secure web browsing sessions
- Use a strong unique password for each financial institution you do business with
- Change your passwords frequently
- Enable SVB Security Alerts & Notifications for SVB accounts
- Set approval limits for sub users on your account
- Log out of online banking sessions after conducting activity in public places
- Utilize thumbprint authentication in the mobile application
- Don't share banking credentials

Immediately notify your SVB Relationship Advisor if you suspect fraudulent activity on your account.