First Republic Bank
It's a privilege to serve you®

Best Practices for Protecting Personal Information

At First Republic, your account security and peace of mind are of the utmost importance. To help you protect your personal financial information, please review the following tips.

Secure your devices

- Ensure you use password protection and lock screens on your smartphones and computers.
- For an added layer of security, don't store bank account information or passwords on your phone.
- Make sure your security software is current.
- Don't open files, click on links or download programs sent by strangers.
- Be wise about Wi-Fi: Avoid sending personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel and other public places.
- Delete personal information before discarding or selling a digital device.

Use unique, strong passwords

- Use different usernames and passwords for your online accounts.
- The longer the password, the harder it is to crack. Create passwords with letters, numbers and special characters.
- Change your passwords often. Mark your calendar to remind you when to update your passwords regularly.

Secure your documents

- Lock up your financial documents and records in a safe place.
- Shred personal documents that you no longer need, such as old receipts, credit offers, credit applications, insurance forms, checks, bank statements, expired credit cards, etc.
- Protect your medical information by destroying labels on prescription bottles before you throw them out.
- Remove cards or documents from your wallet that you don't use regularly, especially your Social Security card and birth certificate.

Be curious and cautious

- Don't respond to emails or phone calls that request your personal information. If you receive an email or phone call asking for any personal details, contact your banker or our client services at (888) 408-0288. A First Republic representative will never call or email to request personal account information.
- Regularly review your bank, credit card and other financial transactions and immediately report any suspicious activity.
- Protect your mail by securing your mailbox, picking up sensitive documents in person, and following up on expected bills or statements that don't arrive.

Follow up with institutions that use your information.

Internal Revenue Service (IRS)

- View and verify your IRS account information to ensure your payout, tax information and payment history are correct.
- You can also request an identity protection PIN to help prevent the misuse of your Social Security number on fraudulent federal income tax returns.
- If you are concerned that you are a victim of identity theft, you can submit an identity theft affidavit to alert the IRS that your account may have questionable activity.

Health insurance

- You can request a Medical Information Bureau consumer file, which will contain a comprehensive medical report based on your personal information. Your detailed prescription history can also be requested through Milliman IntelliScript.
- Review these documents to ensure that your information has not been used to file false medical claims and prescriptions.

Driver's license information

- Fraudsters may sometimes use stolen driver's license numbers to cash bad checks, which can reflect negatively on the driving record of the real owner of the driver's license number.
- To ensure you don't have any bad checks attributed to your driver's license number, you can request a copy of your driving record from the Department of Motor Vehicles. Most states only charge a $10 fee.
- You can also request a free annual consumer report from each of the big three check verification companies, ChexSystems, Certegy and TeleCheck.

For additional tips, visit our online Security and Fraud Prevention Center at:
firstrepublic.com/privacy/security-and-fraud-prevention