Smart practices for everyone

Use smart passwords.

Make sure all passwords are complex and are not repeated across multiple accounts. If available, enable two-factor authentication such as having a one time code sent to your cell phone as part of the sign on process.

Be skeptical.

Scammers are seeking victims through online ads, social media, e-mail, physical mail, and phone calls. Always be skeptical of communication from individuals you don't know. Never divulge personal information to anyone whose identity you can't verify.

Beware of scams.

Any e-mails or phone calls from an entity attempting to solicit personal information are fraudulent. Do not release any information and hang up immediately.

Beware of prize or lottery schemes.

Any e-mails or phone calls telling you you're a winner and requesting your personal information are fraudulent. Remember: you cannot win money in a lottery or competition unless you entered it in the first place. If it sounds too good to be true, it probably is. Do not release any information and hang up immediately.

To contact the three major credit bureaus to request a report or place alerts or freezes on your files:

Equifax – 800-349-9960 or equifax.com

Experian – 888-397-3742 or experian.com

TransUnion – 888-909-8872 or transunion.com

Report any suspicious activity in your Partners Bank accounts.

In Virginia, call 540-899-2265

In Maryland, call 240-776-6204

Or visit **VAPartnersBank.com**

If you believe you are the victim of identity theft, contact your local law enforcement office and/or your state attorney general.

What you need to know about the **Equifax data breach**

VIRGINIA PARTNERS BANK®
MARYLAND PARTNERS BANK®
(a division of Virginia Partners Bank)

What is the Equifax breach?

Equifax, one of the three national consumer credit reporting agencies, announced a major data breach in late summer of 2017. The breach affected over 145.5 million Americans. The Equifax breach gave criminals access to people's personal information such as: names, social security numbers, birth dates, addresses, driver's license and credit card numbers. This information could be used to fraudulently open financial accounts, apply for mortgages or credit cards, file for tax refunds, or even steal your benefits.

Virginia Partners Bank and Maryland Partners Bank were not compromised in this breach. Your information with us remains safe and secure.

We are committed to your financial well-being, and offer this guide to securing your sensitive financial information. We recommend that you follow these suggestions and good practices regardless of whether you have been affected by the Equifax breach.

What should you do?

Since the original release of the Equifax breach in August, the number of affected people has continued to grow. Therefore, we recommend that you assume you were affected and follow our step-by-step process to protect yourself and your financial well-being.

Create a "my Social Security" account.

"my Social Security" allows you to track your future benefits. It's a good idea to set this account up in your name to prevent someone else from claiming it. Do so at ssa.gov/myaccount. *Note: You must set up this account before you freeze your credit file. (See next panel)*

Enable alerts & monitor your accounts.

- **Set up alerts** on ALL your bank and credit card accounts so you'll know about any activity on your accounts. For your accounts with us, you can set up your alerts today at VAPartnersbank.com, or by visiting one of our local branches to have someone help you.
- **Monitor your bank accounts** for fraudulent transactions. View your accounts with us online at any time at VAPartnersBank.com. Whether or not you were affected, closely monitoring your financial information can protect you from identity theft.
- **Monitor your credit reports** by ordering a free copy of your report from each of the three credit reporting agencies. You are entitled to one free report from each bureau per year. Stagger your requests to provide closer monitoring.
- **Consider signing up for a credit monitoring service.** In lieu of relying on free agency reports, you may consider signing up for a service. There are a number of reputable companies which, for a fee, provide continuous monitoring of your credit reports and will inform you of any changes to your credit report.

Consider freezing your credit file.

Freezing your credit file means nobody can open a credit account of any kind in your name. This provides a high level of protection, but may not be advisable if you anticipate needing credit soon. (Before doing so read *Create a "my Social Security" account* in this brochure). There are nominal fees on credit freezes, but they are free for victims of identity theft. A freeze will remain in place until you lift it. To freeze your credit file, contact all three credit reporting agencies.

Consider placing a fraud alert on your credit file.

A fraud alert requires businesses to call you before opening a new account. This extra step may deter fraudsters. Fraud alerts are free, but they expire after 90 days, so you'll need to renew them. You can place a fraud alert by contacting only one of the three credit reporting agencies. That agency will alert the other two.

What to do if you know you are a victim of identity theft.

Report identity theft and create a recovery plan.

If you are a victim of identity theft, visit IdentityTheft.gov. This site is the Federal Trade Commission's resource for identity theft victims and provides checklists and sample letters to guide you through the recovery process.