FORTALICE CLIENT ADVISORY

THE EQUIFAX BREACH: NEXT STEPS TO SECURE YOUR ASSETS

SEPTEMBER 12, 2017

Fortalice

Fortalice

Executive Summary

EQUIFAX: What Now?

It's likely your sensitive information – along with most American consumers - was included in the recent Equifax breach. Fortalice is vigilantly watching for signs of such attacks amongst our customers and this advisory, we recommend 7 key steps for a layered defense:

1. Freeze your Credit Files
2. Sign up for Fraud Alerts
3. Change Passwords
4. Enable Two-Factor Authentication
5. Sign up for Credit Monitoring
6. Regularly Monitor Your Accounts
7. File Your Taxes Early

HOW TO PROTECT YOURSELF

Following the Fortalice Client Advisory issued on September 8th, the action plan below will help you to protect your financial data and sensitive personal information from cyber criminals and also help to better prepare you for the next cyberattack.

Note: If you decide to access the Equifax site to determine if your information was exposed, ensure that you're on a secure computer and using an encrypted network connection before – and any time – you enter your Social Security Number.

1. **Freeze Your Credit Files:** With your sensitive information potentially being sold on the dark web as you read this, you should consider putting a freeze on your credit files. While credit freezes are cumbersome, they are significantly safer than simple credit monitoring, and make it more difficult for someone to open a new account in your name. A credit freeze *won't* prevent a criminal from making charges to your existing accounts. Freezing your credit reports at all three major bureaus, Equifax, TransUnion, and Experian typically cost $3 to $10 per bureau to place and remove. Make sure you keep your credit freeze confirmation letter containing the unique PIN or password - you'll need it if you choose to lift the freeze. If you decide not to place a credit freeze, at least consider placing a **fraud alert** at all three bureaus.
2. **Sign up for Fraud Alerts**: Fraud alerts are free, but they don't lock down your credit. Potential creditors should contact you to verify your identify any time you (or a thief) tries to open a new account. A basic fraud alert expires after 90 days, which means you'll need to be proactive in renewing them. You should also access your free annual credit report to check for any irregularities at annualcreditreport.com.
3. **Change passwords**: Change the passwords to your financial accounts and avoid repurposing the same passwords across multiple accounts. Use a password manager such as LastPass.com to generate random passwords and make them at least 18 characters long. Check the site HaveIBeenPwned.com which will let you know which accounts may have been compromised in other recent breaches.
4. **Enable Two-factor Authentication.** Enabling two-factor authentication (2FA) on every account that supports it. Two-factor provides another layer of defense against a criminal compromising your accounts.
5. **Sign up for Credit Monitoring**: Credit monitoring services don't protect you against identity theft, but they serve as a secondary barrier to exploitation. Whether or not your information was exposed by the breach, you can get a year of free credit monitoring from Equifax –you have until November 21, 2017 to enroll. Keep in mind that many credit-card companies and other financial organizations now offer free monthly or quarterly credit reports.
6. **Regularly Monitor Your Financial Accounts**: The Equifax breach is massive and will have long-term impacts on many consumers. Criminals can be patient – willing to wait until the attention to the breach dies down before they make their move. Just because you don't see any criminal activity on your accounts immediately, doesn't mean you haven't been compromised. Diligently monitoring your accounts and financial statements on a regular basis can enable you to respond immediately to any suspicious activity.
7. **File Your Taxes Early:** File your taxes as soon as you have the necessary information. Criminals may attempt to use stolen social security numbers to file fraudulent tax returns and receive refunds. Prevent this by filing your taxes early. Reference the IRS's guide at https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft for additional information.

HOW TO PROTECT YOUR BUSINESS

The Equifax breach should serve as a critical reminder on the importance of securing your organization's sensitive data. Here are recaps:

1. **Patch Religiously**: An unpatched system leaves your business and data vulnerable to exploitation by hackers. Patch regularly to thwart most attacks.
2. **Educate Employees:** One of the most significant ways to protect data is ensuring your employees understand the risks associated with mishandling it and are consistently working to secure the sensitive information.
3. **Minimize Retention and Access**: Avoid collecting sensitive information that you may not need, ensure that if you do retain it, you also limit the number of personnel with access to the data and purge the information when it is no longer needed.
4. **Conduct Periodic Risk Assessments**: With periodic assessments, you can evaluate new or emerging areas of concern for potential security risks. Also make sure your cybersecurity policies are consistently updated.
5. **Plan Your Incident Response:** Incorporate data loss prevention procedures into your Incident Response Plan and regularly exercise simulated forensics scenarios to enable your team to adeptly respond during high-pressure situations.

CONTACT FORTALICE

If your information was compromised or you want additional information about securing your data, reach out to us at watchmen@fortalicesolutions.com or visit the Identity Theft Resource Center at http://www.idtheftcenter.org for free information and services.