The Equifax Breach – What You Should Know

What Happened?

On September 7, 2017, Equifax announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. The unauthorized access occurred from mid-May through July 2017. See Equifax's statement here.

What Information is at Risk?

The information accessed primarily includes:

- Names
- Driver's license numbers (in some instances)
- Social Security numbers
- Credit card numbers
- Birth dates
- Addresses
- Certain dispute documents with personal identifying information

How Do I Find Out if My Personal Information May Have Been Impacted? How Do I Enroll in Complimentary Identity Theft Protection and Credit File Monitoring Services?

Visit https://www.equifaxsecurity2017.com/enroll and scroll down the page. You will see a button that asks you to "Begin Enrollment." Follow the steps outlined. At the beginning of this process you will find out whether your personal information may have been impacted by this incident.

After that step you will be given a date to return to this site to enroll in TrustedID Premier – this is a complimentary identity theft protection and credit file monitoring service. Be sure to mark your calendars as you **will not** receive additional reminders.

What Else Can I Do to Protect My Identity?

Visit the FTC site for helpful videos and links.

If you believe your identity has been compromised, you can also visit the government site for step-by-step instructions.

How Do I Place a Freeze on My Credit Report if I Think My Data May Be at Risk and What Are the Implications of Doing So?

You will want to do a security freeze on each of the credit bureau sites.
A security freeze will prevent anyone from accessing that credit report. So, if a fraudster is attempting to open a checking account using your info (SSN, DOB, etc.), when the bank or store or whatever goes to pull your credit report, your credit report will return a warning that you will have to contact the credit bureau to proceed with any future application. This will be particularly important in a mortgage application as most lenders use a tri-merge credit report that pulls from each of the three major vbureaus.

1. Complete the freeze for Equifax here. They will give you a 10 digit PIN to use to remove or thaw the freeze. Make sure you store the PIN in a secure place as you will need it in the future any time you authorize someone to run your credit report.

(Continued)

2. Complete the freeze for Experian here. Experian will allow you to set your PIN. Note that in the state of California there will be a $10 fee for freezing your credit.
3. Complete the freeze for TransUnion here. At Trans Union, you have to set up an account to perform the freeze. Their PIN only allows up to 6 digits. TransUnion also requires a $10 fee.
4. Complete the freeze for Innovis here. They will provide you with a 10 digit PIN to manage access to your report for the duration of the freeze. No fee is required.

Each of these places will give you a number you can call to unfreeze or thaw your reports. Whenever you next go to open an account or apply for a loan, you'll have to contact the credit bureau ahead of time (either on the phone or online) and "thaw" your account for a period of time that you determine. You can set the "thaw" either for a period of time or for a particular creditor, aka "Montecito Bank & Trust" or another lender. If you determine you don't want the protection any longer you can remove it. You will need that PIN you set for each of the bureaus to thaw or unfreeze each of your reports.

Finally, if you know you're going to be looking for a car, applying for a mortgage, etc. over the next week, you may call the bureaus and thaw your report for that specific week. Or, if you are applying for a credit card, call and unfreeze your report for that company, and then turn the freeze back on. While it creates an additional step for you, during the "thaw" the fraudster could use your compromised social security number, address and/or date of birth to apply for a loan or open an account.

What Else Can I Do?

Contact your bank for additional security measures:

1. Armed with your personal data, a fraudster could attempt to "phish" for more information, such as your existing bank information. Your financial institution should allow you to establish security questions and answers to allow your banker to verify your identity using something the fraudster isn't likely to have access to, such as the name of your childhood best friend or a favorite book or movie.
2. Check your online banking often, report anything immediately, and close out those accounts.

What is Montecito Bank & Trust Doing to Protect My Information?

Montecito Bank & Trust takes cybersecurity extremely seriously, and the trust of our clients is something we consider vitally important and part of our core banking principles. As a result, earlier this year we moved to a new online banking platform that now requires multi-factor authentication to enroll. In addition, we are active in the cybersecurity space and have materials available at montecito.bank/security. Watch for weekly tips and fraud trends in October as part of National Cybersecurity Awareness month, a national campaign designed to increase the public's awareness of cybersecurity and cybercrime issues.

This is being provided for informational purposes only. Montecito Bank & Trust is not making recommendations of action or inaction. It is important for you to consider what may be the best option for you.