For Immediate Release
September 12, 2017
Contact: Debbie Jemison
217-789-9340

The Illinois Bankers Association Offers These Tips for Navigating the Equifax Data Breach and Protecting Your Personal Information

Equifax ─ one of our nation's three major credit reporting bureaus ─ announced last week that it had been breached. Hackers accessed personal information from over 143 million Americans, including their social security numbers, birth dates, addresses, and in some cases, driver's license numbers. In addition, credit card numbers for more than 200,000 people appear to have been stolen.

Equifax has created a website ─ https://www.equifaxsecurity2017.com ─ where consumers can check to see if their personal information may have been exposed. (*Be sure to access the site from a secure computer!*) Consumers also can call Equifax at 866-447-7559 for more information. Equifax also will be sending a mailing to all consumers who may have had their information stolen ─ however, this could take time.

Below are additional steps that consumers should take.

- Obtain your credit report every year from each of the three major credit bureaus ─ **Equifax**, **Experian**, and **TransUnion**. All consumers are entitled to obtain a **free copy** of their credit report from each of these companies every 12 months. You can do this by visiting www.annualcreditreport.com, or by calling each of them by phone (Experian at 888-397-3742, TransUnion at 800-680-7289, and Equifax at 800-525-6285).

- Consider placing a "credit freeze" on your credit reports with these companies. In most states, including Illinois, each credit bureau may charge you up to a $10 fee for a credit freeze. (Equifax announced on Sept. 12 that it will no longer charge $10 for a security freeze.) A credit freeze prevents lenders and others from accessing your credit information, making it much harder for someone to open a new account of any kind in your name ─ only your current creditors will be able to access your credit report. Also note that you can tell the credit bureaus to lift your credit freeze if you need to apply for new credit, which you can do for a particular credit application or temporarily for a chosen period of time. Keep in mind that a credit freeze won't prevent your creditors from reporting your payments on existing accounts to the credit bureaus.

- Pay close attention to credit card and bank account statements for any unauthorized charges.

- Consider placing a fraud alert on your credit report files. This alert warns creditors that you may be an identity theft victim, and they should take extra steps to verify that anyone seeking credit in your name is really you!

- Consider enrolling in a credit monitoring service. Equifax is offering one free year of credit monitoring to all consumers, regardless of whether your personal information may have been stolen. You can find many other reputable companies that offer this type of service by conducting an Internet search for credit monitoring services.

Know that protecting your personal information is of paramount importance for your bank. All banks are required by law to use a combination of rigorous safeguards to protect their customers' information, including strict privacy policies, encryption, two-factor identification, and extensive employee training. Banks also use sophisticated fraud detection software algorithms that constantly monitor accounts to help flag fraud and identity theft. Your bank invests substantial time and resources to ensure that your accounts and personally identifying information are fully secure.

We also strongly recommend taking these additional precautions to protect your personal information.

Extra Steps for Protecting Your Personal Information

- Never provide personal information, including your password, in response to an unsolicited phone call, website or email request. Some of these requests are now even coming by automated phone messages and mobile phone texts, asking consumers to enter their credit or debit card numbers for some kind of verification.

- If you believe that a request for your personal information may be legitimate, contact the financial institution yourself, rather than responding to the communication.

- Remind your children and elderly relatives to never share their address, telephone number, passwords, social security number, school name or any other personally identifying information.

- Collect your mail promptly. Ask the post office to put your mail on hold, or have a neighbor pick up your mail, when you are away from home for more than a couple of days.

- Shred receipts, bank statements and unused credit card offers, or tear them up before throwing them away.

- If you are conducting business online, make sure that your browser's "padlock" or "key icon" is active, indicating a secure transaction.

- Never open email from unknown sources, and keep your computer up-to-date with virus detection software, anti-spam filters, and bad website blockers.

- When using social networking sites, never include your personal information such as your birthdate, email address, physical address, mother's maiden name, or other information that could provide sensitive information to criminals or hints to passwords.

- Change your website passwords frequently, and never use the same password for multiple websites. Consider using software that acts as a password manager ─ some of

the more popular ones include 1Password, Dashlane, LastPass, RoboForm, and KeePass (which is free).

Importantly, if you suspect your identity has been stolen, immediately call your bank and credit card issuers, so they can begin working on protecting your compromised accounts and clearing your name! Additionally, file a police report, and then contact the three major credit bureaus.

For more assistance, call the Federal Trade Commission's "ID Theft Consumer Response Center" at 1-877-ID THEFT, or go online at www.ftc.gov/idtheft.

The Illinois Bankers Association is a full-service trade association dedicated to creating a positive business climate that benefits the entire banking industry and the communities we serve. Founded in 1891, the IBA brings together state and national banks and savings banks of all sizes in Illinois.

Visit www.ilbanker.com

ILLINOIS BANKERS™

Equifax Breach Frequently Asked Questions

I've been hearing about the Equifax breach in the news. What happened?

Equifax, one of the three major credit bureaus, experienced a massive data breach. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people.

Was my information stolen?

If you have a credit report, there's a good chance it was. Go to a special website set up by Equifax to find out: https://www.equifaxsecurity2017.com/. Scroll to the bottom of the page and click on "Potential Impact," enter some personal information and the site will tell you if you've been affected. Be sure you're on a secure network (not public wi-fi) when you submit sensitive data over the internet.

How can I protect myself?

- **Enroll in Equifax's services.**
  Equifax is offering one year of free credit monitoring and other services, whether or not your information was exposed. You can sign up at https://www.equifaxsecurity2017.com/.

- **Monitor your credit reports.**
  In addition, you can order a free copy of your credit report from all three of the credit reporting agencies at annualcreditreport.com. You are entitled to one free report from each of the credit bureaus once per year.

- **Monitor your bank accounts.**
  We also encourage you to monitor your financial accounts regularly for fraudulent transactions. Use online and mobile banking to keep a close eye on your accounts.

- **Watch out for scams related to the breach.**
  Do not trust e-mails that appear to come from Equifax regarding the breach. Attackers are likely to take advantage of the situation and craft sophisticated phishing e-mails.

Should I place a credit freeze on my files?

Before deciding to place a credit freeze on your accounts, consider your personal situation. If you might be applying for credit soon or think you might need quick credit in an emergency, it might be better to simply place a fraud alert on your files with the three major credit bureaus. A fraud alert puts a red flag on your credit report which requires businesses to take additional steps, such as contacting you by phone before opening a new account.

How do I contact the three major credit bureaus to place a freeze on my files?

Equifax: Call 800-349-9960 or visit its website.

Experian: Call 888-397-3742 or visit its website.

TransUnion: Call 888-909-8872 or visit its website.

Where can I get more information about the Equifax breach?

You can learn more directly from Equifax at https://www.equifaxsecurity2017.com/. You can also learn more by visiting the Federal Trade Commission's web page on the breach at https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do. To learn more about how to protect yourself after a breach, visit https://www.identitytheft.gov/Info-Lost-or-Stolen

Federal Trade Commission
Credit Freeze FAQs

If you're concerned about identity theft, those reported mega-data breaches, or someone gaining access to your credit report without your permission, you might consider placing a credit freeze on your report.

What is a credit freeze?

Also known as a security freeze, this tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your file, they may not extend the credit.

Does a credit freeze affect my credit score?

No. A credit freeze does not affect your credit score.

A credit freeze also does not:

- prevent you from getting your free annual credit report
- keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you're doing any of these, you'll need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it's best to check with the credit reporting company in advance.
- prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Does a credit freeze stop prescreened credit offers?

No. If you want to stop getting prescreened offers of credit, call 888-5OPTOUT (888-567-8688) or go online. The phone number and website are operated by the nationwide credit reporting companies. You can opt out for five years or permanently. However, some companies send offers that are not based on prescreening, and your federal opt-out right will not stop those kinds of solicitations.

As you consider opting out, you should know that prescreened offers can provide many benefits, especially if you are in the market for a credit card or insurance. Prescreened offers can help you learn about what's available, compare costs, and find the best product for your needs. Because you are pre-selected to receive the offer, you can be turned down only under limited circumstances. The terms of prescreened offers also may be more favorable than those that are available to the general public. In fact, some credit card or insurance products may be available only through prescreened offers.

Can anyone see my credit report if it is frozen?

Certain entities still will have access to it.

- your report can be released to your existing creditors or to debt collectors acting on their behalf.
- government agencies may have access in response to a court or administrative order, a subpoena, or a search warrant.

How do I place a freeze on my credit reports?

Contact each of the nationwide credit reporting companies:

- Equifax — 1-800-349-9960
- Experian — 1-888-397-3742
- TransUnion — 1-888-909-8872

You'll need to supply your name, address, date of birth, Social Security number and other personal information. Fees vary based on where you live, but commonly range from $5 to $10.

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze?

In a few states, credit freezes expire after seven years. In the vast majority of states, a freeze remains in place until you ask the credit reporting company to temporarily lift it or remove it altogether. A credit reporting company must lift a freeze no later than three business days after getting your request. The cost to lift a freeze varies by state.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit reporting company the business will contact for your file, you can save some money by lifting the freeze only at that particular company.

What's the difference between a credit freeze and a fraud alert?

A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Three types of fraud alerts are available:

- **Initial Fraud Alert.** If you're concerned about identity theft, but haven't yet become a victim, this fraud alert will protect your credit from unverified access for at least 90 days. You may want to place a fraud alert on your file if your wallet, Social Security card, or other personal, financial or account information are lost or stolen.
- **Extended Fraud Alert.** For victims of identity theft, an extended fraud alert will protect your credit for seven years.
- **Active Duty Military Alert.** For those in the military who want to protect their credit while deployed, this fraud alert lasts for one year.

To place a fraud alert on your credit reports, contact one of the nationwide credit reporting companies. A fraud alert is free. The company you call must tell the other credit reporting companies; they, in turn, will place an alert on their versions of your report.