DATA BREACHES: WHAT TO DO NEXT

Consumer Alert

Data Breaches: What to Do Next

In the news:

The number of data breaches and reported incidents of identity theft continues to set records nearly every year. According to the Identity Theft Resource Center's (ITRC) Annual Review, the number of U.S. Data breaches tracked in 2017 hit a new all-time high of 1,579, up 44.7 percent over last year's record totals of 1,091 breaches.
Additional findings include:

- The number of credit card numbers exposed in 2017 totaled 14,207,346 which was up 88 percent since 2016; and
- More than eight times the number of Social Security numbers were exposed in 2017 than in 2016.

What you need to know:

Stolen personal information is more likely to be used to commit identity theft. On average, there is one identity theft victim in the U.S. every two seconds. And for Michigan consumers, the Federal Trade Commission reports that three of the top 15 metropolitan areas (per capita) for identity theft reports in 2017 are in Michigan–including the number one city: Ann Arbor.

Thus, if your information is impacted, you need to take the threat seriously and take steps to prevent becoming an identity theft victim

This Alert identifies and explains steps you can take to protect yourself and your information following a data breach or security incident.

Data breaches and security incidents

Experts suggest that the most likely thing that will happen to your information after the data breach is that it will be misused in some manner and you will have to resolve that.

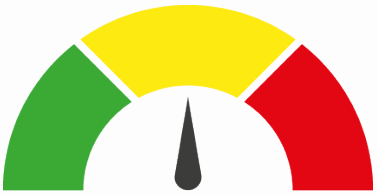
Best case scenario, you will suffer only minor distress and inconvenience and you will resolve it within weeks to a couple months.

Worst case, you ignore the breach, take no action, and you end up the victim of multiple identity-theft incidents that will take you years to clean up.

Even worse: the negative impact hits you at the same time you are trying to secure financing to buy a home, get a car loan, or student loans for college.

Least sensitive

Contact information–name, address, phone number, email address



More sensitive

- **Credit & debit card numbers**
- **Birth dates**
- **Maiden names**
- **Driver's license number**

Most sensitive

- **Social security number**
- **Bank & financial account numbers**
- **Account logins & passwords**

Dana Nessel
Attorney General

DATA BREACHES: WHAT TO DO NEXT

Consumer Alert

Contact information—name, address, phone number, email address

Someone else having this information alone is generally not enough to put you at much risk.

However, thieves use basic contact information as a gateway to get more sensitive personal information, so you need to be on the lookout for phishing emails and calls.

- **Credit & debit card numbers**
- **Birth dates**
- **Maiden names**
- **Driver's license number**

Stolen credit card numbers may result in fraudulent charges. Federal law limits credit card holders' fraud liability to $50 if a thief personally presents your card to make a purchase; and $0 liability if the thief uses your card by phone or the internet.

Stolen debit card numbers can result in overdrafts and bounced checks. Your liability will depend on how quickly you report the theft.

If you notify the card issuer immediately and before the card is used, your liability is $0; it is up $50 if you notify the card issuer within two business days (or 60 days for unauthorized withdraws appearing on your monthly statement); after that, if more than 60 days pass and you have not notified the card issuer, your liability could be unlimited.

Thus, if your credit or debit card numbers are stolen, immediately contact the card issuer.

Someone possessing your birth date information or maiden name, like contact information, is not in itself inherently risky; however, when it is combined with your name and other contact information, it is more valuable to thieves because it never changes and is often asked for to verify identity.

In Michigan, if your driver's license is stolen, go to your local branch with proper ID and ask for a "stolen flash" to be put on your record.

- **Social security number**
- **Bank & financial account numbers**
- **Account logins & passwords**

A stolen social security number is a worse-case scenario. A valid SSN can be sold to undocumented workers or to people trying to hide their identities.

With your social security number and your name, almost anyone can pose as you; open new loans and credit accounts in your name; incur medical debts; create medical records; file fake tax returns; and generate criminal records.

Report the theft of your social security number to the local police; the Social Security Administration (SSA); the Internal Revenue Service; the Internet Crime Complaint Center; and if identity theft results, the Federal Trade Commission.

Immediately report the theft of your bank and financial account numbers.

Stolen account logins and passwords create multiple fraud opportunities for thieves to directly steal from you or search your email for more personal sensitive information.

The damage can multiply if you use the same login and password for other accounts. Change affected logins and passwords immediately; and use two-step authentication.

DATA BREACHES: WHAT TO DO NEXT

Consumer Alert

Steps for consumers who receive notice of a breach or incident

1. **Find out what information was compromised and act accordingly**
2. **Pull your credit report and then check it regularly**

Michigan consumers have the right to order a free credit report from each of the three major credit reporting companies every year.

Consumers can order their free annual credit reports:

- By Mail—Complete the Annual Credit Report Request Form (https://www.annualcreditreport.com/manualRequestForm);
- By Telephone—Call 877-322-8228 (toll free); or
- Online—(annualcreditreport.com, is the only truly free credit report website). **Beware**: Misspelling this site or using another site with similar words will take you to a site that will try to sell you something or collect your personal information.

To maximize your protection against fraudulent activity, order one report from a different company every fourth month. When you order, request that no more than the last four digits of your social security number appear on copies of your credit report.

Review our Alert, Free Annual Credit Reports—What Consumers Should Know, to learn more about what is in your credit report; what you should look for on your credit report; and what to do about errors.

If you are a victim of identity theft, you are entitled to place a fraud alert on your file and to receive copies of your credit report from each credit reporting companies free of charge, regardless whether you have previously ordered your free annual reports.

Requesting a copy of your own credit report is known as a "soft inquiry" and will not affect your credit scores.

3. **Put a fraud alert on your credit file**

A fraud alert is a free alert, or flag, that is placed on your credit file when you notify a credit reporting agency that your information may have been compromised. This alert will make it more difficult for anyone to open an account in your name. The Federal Trade Commission provides a checklist for this.

When you place a fraud alert on your credit report with one agency, federal law requires that agency to notify other nationwide credit reporting agencies, who will then place alerts on your reports with them.

In addition, when you place a fraud alert or credit freeze on your credit report, it will freeze online access to your social security information with the Social Security Administration. Thus, if you have not created an account with social security, you will not be able to do so online unless or until you lift or remove the alert or freeze. To create an account without lifting or removing the alert or freeze, you must go to your local social security office in person with proper identification.

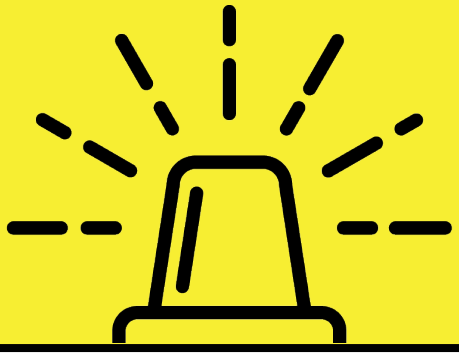
There are three types of fraud alerts:

a. **Initial fraud alert**:

   If you are concerned about or you suspect identity theft, an initial fraud alert can make it harder for an identity thief to open accounts in your name. These alerts last for one year, and may be renewed.

   Anyone requesting your credit file during this year-long window is alerted that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or get a new card on an existing account, the creditor is required to take additional steps to try to verify that you have authorized the request.

   If the creditor cannot verify your authorization, then the request should be denied.



DATA BREACHES: WHAT TO DO NEXT

Consumer Alert

b. Extended fraud alert:

These are for confirmed identity theft victims; last for seven years; and require a police report to verify your identity theft victim status.

In the case of an extended alert, federal law requires that a creditor must call the consumer using the phone number in the alert before authorizing any request to open or modify a credit line.

c. Active duty military alert:

This free fraud alert lasts for one year and is available to active members of the military who want to protect their credit while deployed.

4. Consider a security freeze on your credit file

A security freeze or credit freeze is something you request from a credit reporting agency to restrict access to your credit report.

This makes it more difficult for identity thieves to open new accounts in your name because most creditors will demand to see your credit report before they approve new credit. If a creditor cannot see your file, then the creditor should not extend the credit.

A credit freeze does not prevent all third parties from seeing your report. Existing creditors, debt collectors acting on their behalf, and government agencies in limited circumstances will have access to your report. But placing a credit freeze on your account will not affect your credit score—nor will it keep you from getting your free annual credit report, or from buying your credit report or score.

Credit reporting agencies may not charge a fee to place or to temporarily or permanently lift a security freeze.

5. Credit monitoring

Credit monitoring is a service that tracks your credit report and alerts you whenever a change is made.

This gives you the opportunity to confirm the accuracy of the change and, if needed, contest any inaccuracy.

The specifics of any service will depend on the provider; however, most adverstise they will notify you within 24 hours of any change to your credit report.

The type of changes you can expect to receive alerts about include: hard inquiries, which are made when a credit card or loan application is submitted in your name; new accounts, which generate a note on your report whenever a new credit card or loan is opened in your name; changes to any existing accounts; and address changes.

Some companies extended their services to include non-credit red flags that monitor sex-offender registries, bank-account activity, or payday-loan applications.

Credit monitoring companies may offer "free" trial periods followed by an expensive automatic renewal that can be difficult to cancel.

Credit monitoring services are frequently offered free of charge for one year to individual's whose information was breached.

6. Take advantage of any free services being offered as a result of the breach

Take advantage of any unconditional and free subscription to any credit monitoring, fraud resolution, or other service designed to protect and help you.

Before you accept a free subscription offered to you as a result of a security breach, carefully consider any conditions placed on your acceptance of this subscription.

For example, will you be charged after a short free period? Or will you only get the free subscription if you give up your right to additional legal redress?

DATA BREACHES: WHAT TO DO NEXT

Consumer Alert

7. Use two-factor authentication

For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token (a physical object in user's possession).

This protects your account even if your password is compromised.

As an extra precaution, you may want to choose more than one type of second authentication (e.g., a PIN) in case your primary method (such as a phone) is unavailable.

8. File your taxes early

To minimize your risk of identity theft related tax fraud, file your tax return early—and first. This assures that your return will be accepted by the IRS and the criminal's fraudulent return in your name will be denied. To learn more, read the Attorney General Alert, Tax-Related Identity Theft.

9. Learn more about the different types of identity theft

Educate yourself about the different types of identity theft, including: financial identity theft; governmental identity theft; criminal identity theft; medical identity theft; and child identity theft.

Additional resources on identity theft prevention and resolution

For more information on how to place credit freezes and fraud alerts on your credit reports, please see the Attorney General's Alert, Credit Freeze; Fraud Alert; & Credit Monitoring.

Additional information on identity theft prevention and resolution for Michigan consumers is available on the Attorney General's website.

Michigan consumers may visit the Federal Trade Commission's website devoted to identity theft or call the Federal Trade Commission's ID Theft Hotline at 877-ID-THEFT (877-438-4338).

If you have a general consumer problem, or want to file a complaint:

You may reach the Attorney General's Consumer Protection Division at:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form

Dana Nessel
Attorney General

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern.

Consumer Alerts are not legal advice, legal authority, or a binding legal opinion from the Department of Attorney General.