Data Breach: What To Do If It Happens To You

You just found out from the news or a notification letter that your personal information was part of a data breach – what should you do? You can take a few simple steps to protect yourself from the risk of having your personal information compromised further. Read more to learn what to do and what it means to be affected by a data breach.

Wisconsin Data Breach Law

Wisconsin Stat. § 134.98 requires most businesses operating in Wisconsin that collect personal information about individuals who reside in Wisconsin to notify them if an unauthorized person has acquired their personal information. This law also applies to Wisconsin state government agencies and to cities, towns, villages, and counties.

What personal information is covered?

The law defines personal information to mean an individual's last name and the individual's first name or first initial in combination with and linked to any of the following elements if the element is not publicly available information, and is not encrypted, redacted or altered in a manner that renders the element unreadable:

- Social security number.

- Driver's license number or state identification number.

- Financial account number including a credit or debit card account number or any security code, access code or password that would permit access to the individual's financial account.

- DNA profile.

- Any unique biometric data including fingerprint, voiceprint, retina or iris image, or any other unique physical representation.

Receiving a notification letter

If you have received a letter indicating that you are affected by a data breach, read it carefully. Some letters

offer you free credit monitoring services. Credit monitoring can assist you in watching your account activity for a period of time when you may be more vulnerable. If you receive a letter that offers it, take advantage of the free monitoring services. Contact the business using contact information you have for them to verify that the letter is legitimate, as you will be giving personal information to initiate monitoring services. Some letters may offer a short period of time to respond before the offer for free services expires. Note, if you are affected by a data breach it does not necessarily mean you are a victim of identity theft.

What to do

- Place a fraud alert on your credit report

- Notify the fraud department of one of the three credit reporting agencies; Experian, Equifax, or TransUnion to request a fraud alert on your credit report. When you request a fraud alert from one bureau, it will notify the other two for you. Your credit file will be flagged with a statement that says you may be a victim of fraud and that creditors should take additional steps to verify your identity before extending credit. A Fraud Alert is free and can be done over the phone or online. The credit reporting agency will request your social security number in order to be sure you are you. A fraud alert can be removed by a consumer by

writing to the credit reporting agency and requesting removal. A fraud alert will remain on record for one year or can be extended for seven years if you send proof, like a police report, that you are a victim of identity theft. You can use the contact information provided here to feel safe when giving them your information.

Equifax Info. Services LLC
(800) 685-1111
www.equifax.com

Experian
(888) 397-3742
www.experian.com

TransUnion
(888) 909-8872
www.transunion.com

Consider placing a security freeze on your credit report instead of a fraud alert

A security freeze is stronger than a fraud alert because it remains in place until you release it and requires that you be alerted if an account in your name is requested. The security freeze must be requested by contacting each of the three credit reporting companies directly. You will be given instructions on how to lift the security freeze in order for you or a creditor to access your credit report. There is no fee to place or lift the security freeze.

Equifax Info. Services LLC
(800) 685-1111
www.equifax.com

Experian
(888) 397-3742
www.experian.com

TransUnion
(888) 909-8872
www.transunion.com

Report theft to the police

If you believe you are a victim of identity theft, contact your local police department and file a report, even if the theft might have happened at some other place. You should request a copy of the report since you will

need it when dealing with your financial institution, credit card issuers, and others.

Check your credit report regularly

Obtain your credit report free from each of the three major credit reporting companies each year. Credit reports contain a wealth of information about a consumer's financial history and checking them regularly is one of the best ways to protect against identity theft. If you notice a credit card or bank account that you do not think you have, it might mean that an identity thief is at work. You can obtain your free credit report from Equifax, Experian, and TransUnion by calling toll-free to (877) 322-8228 or online at www.annualcreditreport.com. By ordering one report from one of the reporting agencies every 4 months, you can get your free credit report 3 times per year.

Contact your local Social Security Administration Office

Ask about obtaining a Social Security statement which shows a listing of your annual earnings by year, along with potential Social Security monthly benefits at retirement. If your annual earnings on this report do not match with what you know your earnings to be, it might indicate that someone is using your Social Security number for purposes of employment. You can also get your Social Security statement online by creating an account at https://www.ssa.gov, and then using their online services to request a statement.

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture, Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
PHONE: (800) 422-7128   TTY: (608) 224-5058

IDTheftStepsForDataBreach640 (rev 10/23)