Notice of Data Event

The Carlson Law Firm ("Carlson" or "we") is providing notice to potentially impacted individuals of a recent cybersecurity event. There is no evidence that any personal information has been misused. The security of personal information is very important to us, and we sincerely apologize for any inconvenience this may cause.

What Happened?

Carlson identified suspicious activity associated with its network. As soon as we became aware of the activity, we took immediate steps to secure our environment and engaged independent computer forensic experts to assist with an investigation. The investigation found that an unauthorized actor accessed our network and may have taken documents stored on the network during the incident. These documents are not part of our current case management or active data storage systems and were maintained separately from the systems we currently use to manage client matters and records. The information stored on the server was complex and not easily searchable but may have included personal information related to certain represented clients.

The type of information impacted includes names, and some combination of the following: addresses, dates of birth, Social Security numbers, driver's license numbers or other government-issued IDs, health treatment and diagnosis, and invoices for healthcare treatment.

Again, we have no evidence of any misuse of the information but are providing notice out of an abundance of caution. We have enhanced our information security program by implementing additional controls, such as deploying end point detection software across our systems, changing all user and system passwords, and tightening access controls.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft by reviewing bank and other financial statements and immediately contacting your financial institution if you identify any suspicious activity. You can also visit the Federal Trade Commission's website for more information on protecting your identity at consumer.ftc.gov/identity-theft-and-online-security.

For More Information:

For more information on steps you can take to protect your information, please see the recommendations provided below. While we have no reason to believe any personal information has been misused, we want to apologize for any inconvenience this may cause.

If you have additional questions or concerns, please contact us at *notification@carlsonattorneys.com* or call 855-292-1148. Emails will be answered within two business days and calls will be answered between 8:00am and 5:00pm, Central Time, Monday through Friday.

Recommended Steps to Help Protect Your Information:

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of

your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the Federal Trade Commission. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.