



1900 M Street NW, Suite 250
Washington, DC 20036

Phone: (202) 296-3585
Website: www.zwillgen.com

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us
By email

April 14, 2023

Dear Attorney General Brown:

On behalf of our client, Essendant Co., we write to provide you with this notification of an incident that affected the personal information of one (1) Maryland resident.

Essendant experienced a ransomware attack on March 6, 2023. Upon learning of the attack, we promptly engaged a team of cybersecurity experts to help our investigation and remediation efforts. In the course of our investigation, we discovered that information relating to a certain Essendant employee had been subject to unauthorized access and potentially made available on the “dark web.” The information was contained in an individual, unsecured file on an Essendant-issued device; Essendant’s HRIS system was not affected by this incident.

The data elements that were accessed without authorization include the employee’s medical information contained in a doctor’s note.

Essendant is notifying the Maryland resident affected by this incident by mail and offering them one year of complementary credit monitoring and identity theft protection services. A copy of the letter sent with identifying information removed is attached for your reference.

Should you have further questions about this matter, please do not hesitate to contact me at 202-706-5226 or marci@zwillgen.com.

Sincerely,
Marci Rozen
Senior Legal Director, ZwillGen PLLC



April 14, 2023

[Name]

[Address]

NOTICE OF DATA BREACH

Dear [Name]:

We are writing to notify you of an incident that may have affected the confidentiality of your personal information. Please read this letter carefully for more information and to learn how you can take steps to protect your personal information, including by enrolling in a complimentary year of Allstate Identity Protection.

What Happened?

As you know, Essendant experienced a ransomware attack on March 6, 2023. In the course of our investigation of this incident, we discovered sensitive personal information about you had been subject to unauthorized access and had potentially been made available on the "dark web." We believe this sensitive personal information was contained in an individual, unsecured file on an Essendant-issued device; Essendant's MyHRIS system was not impacted by this incident.

What Information Was Involved?

The data elements affected by this incident may have included your medical information contained in a doctor's note.

What We Are Doing.

Upon learning of the ransomware attack, we promptly engaged a team of cybersecurity experts to help our investigation and remediation efforts. We are also providing you with one year of complimentary access to Allstate Identity Protection. Additional Information on the services and instructions on how to enroll have been sent to you at your Essendant email address.

What You Can Do.

In addition to enrolling in the Allstate Identity Protection, we recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please see the attachment to this letter.

For More Information.

If you have any questions regarding this incident or if you desire further information or assistance, please contact privacy@essendant.com. We regret any inconvenience caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to read 'Marsha Rubin', with a stylized, flowing script.

Marsha Rubin
Senior Vice President & General Counsel
Essendant

SUPPLEMENTAL INFORMATION

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax P.O. Box 740241 Atlanta, GA 30374 www.equifax.com 1-800-685-1111	Experian P.O. Box 2002 Allen, TX 75013 www.experian.com 1-888-397-3742	TransUnion P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-916-8800
---	--	--

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
--

You may contact and obtain information from and/or report identity theft to your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300.

You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Security Freeze P.O. Box 2000 Chester, PA 19016 www.transunion.com	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 www.equifax.com
--	--	---

To request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- If you have moved in the past five years, provide the addresses where you have lived over the prior five years
- Proof of current address such as a current utility bill or telephone bill
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.

- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.