

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JASON M. GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

NICHOLAS J. MARTIN
nmartin@c-wlaw.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

December 6, 2023

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Breach Notification

To Whom It May Concern:

We serve as counsel for Casto Technical Services ("Casto") located at 540 Leon Sullivan Way, Charleston, West Virginia 25301. By providing this notice, Casto does not waive any rights or defense under Maryland law including the data breach notification statute.

On July 3, 2023, Casto discovered suspicious activity associated with certain Casto systems. Upon discovery, Casto took immediate steps to secure the network and systems, including engaging third-party forensic specialists to assist in a thorough investigation into the nature and scope of the incident. The investigation determined that an unknown party acquired certain information on the Casto network. Casto then began a thorough review of the affected data to determine the type of information potentially affected and to whom the information related. On or around September 21, 2023, Casto completed its initial review and identified limited personal information which may have been impacted. Casto subsequently worked to obtain up to date contact information to provide individuals with direct notification. This process, including a National Change of Address ("NCOA") search, was completed on November 22, 2023. Upon completion of the NCOA, Casto confirmed that this incident potentially affected information relating to three (3) Maryland residents, including their first and last name, date of birth, Social Security number and financial account information.

In response to this incident, Casto took steps to secure their environment, conducted a thorough investigation and notified law enforcement. Additionally, Casto began providing notice to the potentially impacted individuals on December 6, 2023, via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, Casto is offering potentially impacted individuals complimentary credit monitoring and identity theft protection services for 12 months.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:


Jason M. Goodwin, Esq.

Exhibit A



540 Leon Sullivan Way
Charleston, West Virginia 25301

<<Mail ID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>,

We are writing to inform you of a recent incident experienced by Casto Technical Services (“Casto”), which may have impacted certain information we hold on our systems. We take this incident very seriously and are providing you information about the incident, our response, and steps you can take to protect your information out of an abundance of caution.

What Happened? On July 3, 2023, Casto experienced a network disruption incident which affected our ability to access certain systems. We immediately took steps to secure our network and began an investigation, which included working with third-party specialists to assist in our investigation to determine the nature and scope of the incident. Our investigation revealed that certain information within our systems was subject to unauthorized access. We immediately began a thorough and time intensive review of the affected data to determine the types of information that were potentially impacted and to whom it relates. This review was completed on or around September 26, 2023, and we immediately initiated efforts to obtain up-to-date address information for all potentially affected individuals to provide direct notice. On November 22, 2023, this process was completed, and we worked to provide you with this notification as soon as possible.

What Information Was Involved? The information potentially impacted during the incident may have included your first and last name in combination with the following data element(s): <<Breached Elements>>.

What We Are Doing. Upon learning of this incident, we immediately took steps to secure our systems and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you complimentary credit monitoring and identity protection services for a period of <<CM Duration>> months.

What You Can Do. We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft should you feel it appropriate to do so.

For More Information: Should you have any questions or concerns regarding this incident, please contact our dedicated assistance line at 877-880-8983. Casto Technical Services can also be contacted by mail at 540 Leon Sullivan Way, Charleston, West Virginia, 25301.

Sincerely,

Casto Technical Services

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Equifax® Credit Watch™ Gold provides you with the following key features:

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the Equifax website at **www.equifax.com/activate** and enter the Activation Code <<**Activation Code**>> and follow the provided steps to receive your credit monitoring service online.
 - **Register:** Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4
 - **Create Account:** Enter your email address, create a password, and accept the terms of use.
 - **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
 - **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling.
- To sign up for US Mail delivery, dial **1-855-833-9162** for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only. You will be asked to enter your Activation Code home telephone number, home address, name, date of birth and Social Security Number. You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment. Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which

provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

You can sign up for the online or offline credit monitoring service anytime between now and **January 31, 2024**. Due to privacy laws, we cannot register you directly. Enrolling in this service will not affect your credit score. You must be over age 18 with a credit file activate these services.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended fraud alert on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a credit freeze on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.