

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN FARALLY
mfarally@c-wlaw.com

JORDAN MORGAN
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

March 17, 2022

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Security Breach Notification

To Whom It May Concern:

I serve as counsel for Collaborative Effort to Reinforce Transition Success, Inc. ("C.E.R.T.S")¹, located at 52 Reads Way, New Castle, DE 19720. We write to provide notification of a recent data security incident. By providing this notice, C.E.R.T.S does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about November 4, 2021, C.E.R.T.S fell victim to a sophisticated ransomware attack. Upon discovery, C.E.R.T.S immediately secured its network and engaged a third-party forensic firm to investigate the incident. On February 16, 2022, following a thorough investigation, C.E.R.T.S confirmed that a limited amount of personal information may have been impacted by this event. At that time, C.E.R.T.S engaged in a thorough review of the impacted data to identify all potentially impacted individuals.

On March 10, 2022, C.E.R.T.S discovered that ten (10) residents of Maryland were potentially impacted by this incident. We will provide supplemental notification should we determine additional residents of Maryland are potentially affected.

C.E.R.T.S provided notice to the potentially impacted individuals via First Class Mail on March 16, 2022, and is offered the affected Maryland residents complimentary credit monitoring

¹ C.E.R.T.S is a Healthcare Covered Entity under the Health Insurance Portability and Accountability Act ("HIPAA"). See, 45 CFR 164.410.

for 12 months. A copy of the draft notification letter is attached as **Exhibit A**. The letter outlines the incident and provides potentially affected individuals with additional resources to protect their identity and monitor their credit history and personal accounts. C.E.R.T.S is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident. This includes providing notice to the U.S. Department of Health and Human Services in accordance with the HIPAA Breach Notification Rule² and all applicable state regulators.

Please contact me should you have any questions.

Very truly yours,



Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

² See, 45 CFR 164.400-414.

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name >>:

C.E.R.T.S. Adult Action Centers writes to notify you of an incident that may affect the privacy of certain information provided to us. This letter includes information about the incident, our response, and resources we are making available to you.

On or about November 4, 2021, our organization was targeted by a sophisticated ransomware attack that impacted our ability to access certain files on our computer network. In response, we notified law enforcement and immediately engaged a team of third-party specialists to investigate and determine the nature and scope of the incident. Our investigation determined that certain segments of our network were accessed during the incident without authorization. Therefore, we began a thorough review of the information present in the limited network locations impacted by this incident to determine the type of information contained therein and to whom the information relates.

The investigation determined that certain files containing your information may have been accessed during this incident. The information impacted may include your name and <<Breach Elements>>. Additionally, if you were enrolled in the C.E.R.T.S. employee health plan between 2011 and 2021, your health insurance information may also have been impacted. While we have no evidence of actual or attempted misuse of any information as a result of this incident, in an abundance of caution, we are providing you access to complimentary credit monitoring and identity protection services for 12 months. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed "Steps You Can Take to Help Protect Your Information."

Should you have any questions or concerns regarding this matter, please do not hesitate to contact Michelle Shorter, Operations and HR Manager at 302-731-0301 x101, mshorter@certsinc.org, or by writing to us at 52 Reads Way New Castle, DE 19720.

We take the protection of information in our care very seriously and regret that this incident occurred. We greatly appreciate your support and patience while we continue our response to this incident, and we apologize for any concern or inconvenience.

Sincerely,

Vivian J. Turner, MPA
Executive Director

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

We encourage you to always remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements 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.

1. Enroll in Credit Monitoring / Identity Protection

Enrollment Instructions

Go to www.equifax.com/activate and enter your unique Activation Code of <<Activation Code>> no later than <<Enrollment Deadline>>, then click “Submit” and follow these 4 steps:

1. **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.
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling. The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications 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 alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- 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 theft (conditions apply).

2. Place a Fraud Alert or Security Freeze on Your Credit File

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
---	---	--

3. 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. This notice has not been delayed by law enforcement.

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 www.oag.state.md.us. C.E.R.T.S. Adult Action Centers may be contacted 52 Reads Way New Castle, DE 19720.