

WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

7 ST. PAUL STREET
BALTIMORE, MD 21202-1636
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

January 26, 2022

**Privileged and Confidential
VIA EMAIL AND FIRST CLASS MAIL**

Attorney General Brian E. Frosch
Office of the Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Security Breach Notification

Dear Attorney General Frosch,

We are writing on behalf of our client, Girl Scouts of Connecticut (located at 340 Washington St., Hartford, CT 06106), to notify you of a data security incident involving one (1) Maryland resident.¹ Girl Scouts of Connecticut is a nonprofit organization with a focus on providing education, mentorship, and programming to girls throughout Connecticut.

Nature

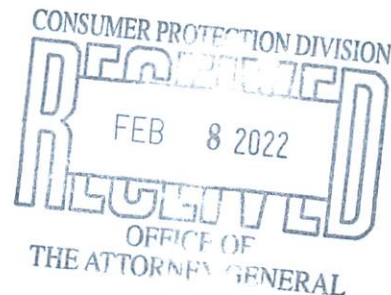
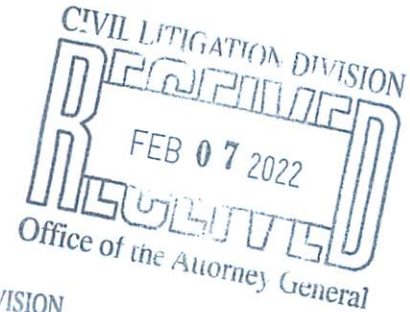
On October 21, 2021, Girl Scouts of Connecticut discovered that it was the victim of a sophisticated cyber incident that impacted its networks and servers which contained protected personal information. After discovering the incident, Girl Scouts of Connecticut took steps to secure and safely restore its systems. Further, Girl Scouts of Connecticut engaged our firm and third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and assist in the remediation efforts. Girl Scouts of Connecticut also contacted the FBI to seek assistance and guidance as one of the many organizations confronting the impacts of the evolving cyber threat landscape.

During its investigation and review, Girl Scouts of Connecticut determined certain data potentially involved in the incident contained personal information. On January 7, 2022, Girl Scouts of Connecticut identified one (1) Maryland resident who had personal information potentially involved in the incident.

The personal information obtained potentially included name and medical and health insurance information.

Notice and Girl Scout of Connecticut's Response to the Event

¹ By providing this notice, Girl Scouts of Connecticut does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland's data event notification statute, or personal jurisdiction.



On January 27, 2022, Girl Scouts of Connecticut will mail a written notification to the potentially affected Maryland resident, Md. Code Ann., Com. Law § 14-3504, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Girl Scouts of Connecticut is providing the potentially impacted individuals with notice of the incident and:

- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, Girl Scouts of Connecticut provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary). Finally, Girl Scouts of Connecticut is working to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A



Girl Scouts of Connecticut
Central Office
340 Washington St.
Hartford, CT 06106
860-522-0163
Fax 860-548-0325

Parent or Guardian of
<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

<date>

Re: Notice of Data Breach

Dear Parent or Guardian of <First Name> <Last Name>

At Girl Scouts of Connecticut, we value transparency and respect the privacy of the above-named minor's information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve the above-named minor's personal information. This notice describes what we did in response, and steps you can take to protect against possible misuse of their personal information.

What Happened

On October 21, 2021, we discovered a ransomware incident that impacted our networks and servers.

After discovering the incident, we quickly took steps to secure and safely restore our systems and operations. Further, we engaged outside counsel and third-party forensic experts to assist in the remediation efforts and conduct a thorough investigation of the incident's nature and scope. We also contacted the FBI to seek assistance and guidance, as one of the many organizations confronting the impacts of the evolving cyber threat landscape.

Concurrent to the investigation, we began a comprehensive review of the information that might be involved. On January 7, 2022, we concluded our initial review and determined that the impacted information could potentially include their personal information. *However, we have no evidence indicating that any information has been used for identity theft or financial fraud.* Regardless, we wanted to notify you of the incident out of an abundance of caution and provide you with information on steps you can take to help protect their information.

What Information Was Involved

The impacted information could potentially involve their medical and health insurance information.

What We Are Doing

As explained above, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating that the above-named minor's information has been used for identity theft or financial fraud, we strongly recommend that you remain vigilant, monitor and review all of their financial and account statements (if applicable), and report any unusual activity to the institution that issued the record and law

enforcement. In addition, please see “***OTHER IMPORTANT INFORMATION***” on the following pages for guidance on how to best protect your identity.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have additional questions, please contact us by calling 860-522-0163, emailing customercare@gsofct.org, or writing to us at 340 Washington St, Hartford, CT 06106.

Sincerely yours,

Diana Mahoney

Diana Mahoney, CEO

* Services marked with an “*” require an internet connection and e-mail account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Minor's Credit Report. We recommend that you obtain a free copy of your minor's credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Alternatively, you can elect to purchase a copy of your minor's credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax (888) 766-0008 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	Experian (888) 397-3742 P.O. Box 2104 Allen, TX 75013 www.experian.com	TransUnion (800) 680-7289 P.O. Box 1000 Chester, PA 19016 www.transunion.com
--	---	---

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your minor's credit report may delay, interfere with, or prevent the timely approval of any requests you or they make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	TransUnion Security Freeze & Fraud Victim Assistance Dept. P.O. Box 6790 Fullerton, CA 92834 https://www.transunion.com/credit-freeze
---	---	--

Consider Placing a Fraud Alert on Your Minor's Credit Report. You may want to consider placing a fraud alert on your minor's credit report. An initial fraud alert is free and will stay on their credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your minor's report and requests that the creditor contact you before establishing any accounts in your minor's name. To place a fraud alert on their credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Remain Vigilant, Review Your Minor's Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your minor's account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf/0009_identitytheft_a_recovery_plan.pdf.

Iowa residents may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa*, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents**: State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **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, the 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 credit. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, <https://ag.ny.gov/internet/resource-center> and or *NYS Department of State's Division of Consumer Protection*, (800) 697-1220, <https://www.dos.ny.gov/consumerprotection>. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/identity-theft/>, or by contacting the Attorney General by calling 1-877-566-7226 or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.