



Richard Goldberg, Partner & Vice-Chair
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
rgoldberg@constangy.com
Mobile: 917.744.1760

October 8, 2024

VIA Email

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Tel: 410-576-6491

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Sterling Corporation ("Sterling") an electronics assembly manufacturing company located in Connecticut, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

1. Nature of the Security Incident

On September 12, 2024, Sterling learned that information related to its employees may have been accessed by an unauthorized person. On July 18, 2024, Sterling discovered suspicious activity that disrupted access to part of its network. Sterling immediately took systems offline and engaged cybersecurity to secure its network and investigate what happened. That investigation eventually revealed that an unauthorized person may have gained access to some personal information belonging to current and former employees. Sterling then worked to ascertain the identities of the potentially involved individuals, the types of their information that may have been involved in this incident, and to locate current contact. This work was completed on September 12, 2024.

To date, Sterling has no reason to believe that personal information of the individuals involved has been misused as a result of this incident. Out of an abundance of caution, Sterling has mailed notifications to all individuals involved, providing them with steps they can take to protect their personal information, and offering them free identity monitoring services.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for one (1) Maryland resident. The information involved in the incident included the individual's name and Social Security number. Again, Sterling has no reason to believe that the information involved has been or will be misused.

3. Notification to the Affected Individual

On October 7, 2024, a notification letter was sent to the affected Maryland resident by USPS First Class Mail. The notification letter provides resources and steps the individual can take to help protect their information. The notification letter also offers twelve (12) months of complimentary identity protection services including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

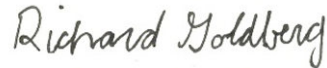
4. Measures Taken to Address the Incident

Sterling terminated the unauthorized access on its network and began an investigation into what happened. Sterling has sent notice to the potentially affected individuals and is providing them with steps they can take to protect their personal information as discussed above. Sterling is also examining its cyber environment in order to consider what steps might prevent a similar incident from happening in the future.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at RGoldberg@constangy.com or 917.744.1760.

Sincerely,



Richard Goldberg
Constangy, Brooks, Smith & Prophete LLP

RG:KD

Encl.: Sample Notification Letter

cc: Kim Detwiler, Constangy (kdetwiler@constangy.com)



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

October 7, 2024

Subject: Notice of Data << Variable Data 1: Security Incident/Breach>>

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

Sterling Corporation ("Sterling") is writing to inform you of a recent data security incident that may have affected your personal information. We take the privacy and security of all personal information within our possession very seriously. This letter contains information regarding the incident and steps you can take to help protect your personal information.

What Happened. On July 18, 2024, we discovered suspicious activity that disrupted access to certain parts of our cyber network. We immediately took systems offline and engaged experts to help us secure the network and investigate what happened. On September 12, 2024, we learned that your personal information may have been involved in connection with an incident. Although we have no information that anyone's data has been misused, we are providing free identity protection to individuals whose information may have been involved in the incident.

What Information Was Involved. The information involved may have included your name and Social Security number.

What We Are Doing. As soon as we discovered the incident, we took the steps described above and attempted to minimize the risk of a similar incident occurring in the future.

We are also offering you access to identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<Membership Offering Length: 1 year/2 years>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To enroll in the services provided through IDX, please scan the QR above, call 1-800-939-4170 Monday through Friday from 9:00 am – 9:00 pm Eastern Time, or visit <https://app.idx.us/account-creation/protect> and insert the Enrollment Code provided above. Please note the deadline to enroll in these complimentary services is January 7, 2025. To receive credit monitoring services, you must be over the age of 18 and have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the IDX identity protection services, which are offered at no cost to you.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call please call IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time.

We take this event and the security of information in our care seriously. We regret any concern or inconvenience that this incident may cause you.

Sincerely,

Sterling Corporation
20 Industrial Ave
Chelmsford, MA 01824

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). 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 Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major 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 print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional Information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; <https://oag.dc.gov/>

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; <https://www.marylandattorneygeneral.gov/>

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; <https://ncdoj.gov/>

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Rhode Island: The total number of individuals receiving notification of this incident is 2. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; <https://ago.vermont.gov/>