



Todd M. Rowe, Partner  
Cybersecurity & Data Privacy Team  
300 S Wacker Drive, Suite 1050  
Chicago, IL 60606  
[trowe@constangy.com](mailto:trowe@constangy.com)  
Mobile: 312.520.2521

March 1, 2024

**VIA ONLINE SUBMISSION**

Attorney General Aaron Frey  
Office of Attorney General  
Consumer Protection Division  
Security Breach Notification  
111 Sewall Street, 6th Floor  
Augusta, ME 04330

Re: **Notice of Data Security Incident**

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Spaulding Clinical Research, LLC (“Spaulding Clinical”) 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 Maine’s data breach notification statute.

**1. Nature of the Security Incident**

On November 8, 2023, Spaulding Clinical became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, it immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. While that investigation is ongoing, Spaulding Clinical has determined that an unauthorized third party accessed and acquired certain files stored in its network, some of which contained personal information for current and former Spaulding Clinical employees. On February 8, 2024, Spaulding Clinical confirmed that personal information for certain employees and beneficiaries was impacted, and then moved as quickly as possible to notify the potentially affected individuals.

**2. Number of Affected Maine Resident(s) & Information Involved**

The incident involved personal information for approximately one (1) Maine resident. The information involved in the incident for affected the Maine resident may have included name and Social Security number.

### **3. Notification to Affected Individual(s)**

On March 1, 2024, a notification letter was sent to the affected Maine resident by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The notification letter also offers the individual whose Social Security number was affected by this event the opportunity to enroll in 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 sent to the impacted individual is included with this correspondence.

### **4. Steps Taken Relating to the Incident**

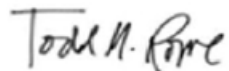
In response to the incident, Spaulding Clinical retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Spaulding Clinical also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

Finally, Spaulding Clinical is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

### **5. Contact Information**

If you have any questions or need additional information, please do not hesitate to contact me at [trowe@constangy.com](mailto:trowe@constangy.com) or 312.520.2521, or David Rice at or [drice@constangy.com](mailto:drice@constangy.com) or 718.614.2656.

Best regards,



Todd Rowe  
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter



Return to IDX:  
P.O. Box 989728  
West Sacramento, CA 95798-9728

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:





Or Visit:

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

March 1, 2024

Subject: Notice of Data <<Variable Text 2>>:

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

We are writing to inform you of a data security incident experienced by Spaulding Clinical Research, LLC (“Spaulding Clinical”) that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

**What Happened:** On November 8, 2023, Spaulding Clinical became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, we immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. While that investigation is ongoing, we have determined that an unauthorized third party accessed and acquired certain files stored in our network, some of which contained personal information for current and former Spaulding Clinical employees. On February 8, 2024 we determined that your information may have been impacted, and moved as quickly as possible to provide notice and resources to assist.

**What Information Was Involved:** The information involved in this incident may have included your name and <<Variable Text 1>>.

**What We Are Doing:** As soon as we discovered this incident, we took immediate steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our network security and reduce the risk of similar future incidents.

We are also providing you with the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: <<12/24 months>> of credit<sup>1</sup> and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that the deadline to enroll is June 1, 2024.

---

<sup>1</sup>To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

**What You Can Do:** We encourage you to enroll in the credit monitoring and identity protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter which includes additional resources you may use to help protect your information.

**For More Information:** Spaulding Clinical has engaged a special call center to help answer your questions about the incident and services being offered. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Central time, Monday through Friday, excluding holidays. To enroll, please call the call center toll-free at 1-888-867-4002 and provide the representative with your unique code listed above, or scan the QR code above or visit <https://app.idx.us/account-creation/protect>.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jeffrey A. Sanchez', written in a cursive style.

Jeffrey A. Sanchez  
Director of Information Technology  
Spaulding Clinical Research, LLC  
525 South Silverbrook Drive  
West Bend, Wisconsin 53095

## STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL 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 FTC 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](http://www.consumer.ftc.gov), [www.ftc.gov/idtheft](http://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](http://www.equifax.com).*

*Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com).*

*TransUnion, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, [www.transunion.com](http://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 FTC 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 [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.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.

**LCS Financial Services Contact Information:** 6782 S. Potomac St., Centennial, CO 80112; 1.866.662.9087

**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](mailto:oag@dc.gov)

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

**Maine:** Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

**Maryland:** Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; [oag@state.md.us](mailto:oag@state.md.us) or [IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

**North Carolina:** 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; [www.ncdoj.gov](http://www.ncdoj.gov)

**New York:** 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/>

**Oregon:** Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, [www.doj.state.or.us](http://www.doj.state.or.us)

**Rhode Island:** Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>. The total number of Rhode Island residents receiving notification of this incident is 0.

**Texas:** Texas Attorney General can be reached at: 300 W. 15<sup>th</sup> Street, Austin, Texas 78701; 800-621-0508; [texasattorneygeneral.gov/consumer-protection/](http://texasattorneygeneral.gov/consumer-protection/)

**Vermont:** Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; [ago.info@vermont.gov](mailto:ago.info@vermont.gov)