Notice of the Langdon & Co. LLP, CPAs Data Security Incident

Date: August 1, 2025

Langdon & Company LLP ("Langdon") is a Certified Public Accounting firm based in Garner, NC that provides tax preparation and auditing services to its clients. Langdon provides financial and accounting services to Easterseals North Carolina & Virginia ("Easterseals"), which requires Langdon to receive certain information regarding Easterseals patients. This notice provides information about a recent data security event Langdon experienced involving some of this information Langdon received from Easterseals.

What Happened? On April 28, 2024, Langdon detected unusual activity on its network. We promptly launched an investigation with the assistance of cybersecurity experts and took immediate steps to secure our systems. Our investigation determined that certain files were taken from our network without authorization between April 21-28, 2024. We then undertook a comprehensive and thorough review of the impacted files, through which we determined that certain files we received from Easterseals may have been impacted. This required extensive analysis to determine exactly which documents belonged to Easterseals, what information they contained, and whose data was involved. We finalized our findings and notified Easterseals of the results on June 3, 2025. Thereafter, we worked to verify the accuracy of the information identified and retrieve mailing information. While we do not have evidence of misuse of anyone's information to date, we worked diligently to notify all potentially impacted people as soon as possible out of an abundance of caution.

What Information was Involved? The types of information identified through our review significantly varied by individual but includes name, address, date of birth, Social Security number, Taxpayer Identification number, financial account numbers, medical information, health insurance information, and/or digital signatures.

What Langdon Is Doing. Upon discovery of the activity on our network, we partnered with computer forensic specialists to investigate the nature and scope of the incident. We notified federal law enforcement and commenced a thorough review of the impacted files to determine who and what was impacted. We have updated our security measures following the incident and are working to update protections for any personal information we are required to store pursuant to applicable law and destroying any information that we are no longer required to maintain. Langdon is providing complimentary credit monitoring and identity theft protection services to impacted individuals.

What You Can Do. In general, individuals should remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, health care provider, and/or financial institution. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

For More Information. For questions on this notice, you may write to Langdon at 223 US-70 Pointe, Suite 100, Garner, NC 27529. You may also contact our dedicated assistance line at 1-833-353-9950 between 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-378-4329	1-888-397-3742	1-800-916-8800
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Prevent Tax Fraud. Now anyone who can verify their identity can obtain an IRS identity protection PIN (IP PIN), not just those who have been victims of IRS identity theft. Even better, the IP PIN can be applied for online at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin without CPA assistance in just 10 minutes. The IP PIN is valid for one year until which the IRS will automatically assign you a new IP PIN for the following year. Please feel free to contact me for assistance applying for your IP PIN online. Some individuals (under certain income caps) who can't apply online (for example, because they can't properly verify their identity through the online process which involves uploading ID copies and taking a selfie) can use Form 15227 to apply for an IP PIN.

Protecting Your Medical Information. As a general matter, the following practices can help to protect you from medical identity theft. Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care. Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date. Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize. For more information about these practices please visit consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Obtain Additional Information about how to avoid identity theft from the Federal Trade Commission, 600 Pennsylvania Ave. NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes. This notification has not been delayed by law enforcement.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or 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. 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.