Maria Efaplomatidis, Partner
Cybersecurity & Data Privacy Team
45 Main Street, Suite 206
Brooklyn, NY 11201
mefaplomatidis@constangy.com
917.414.8991

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

May 29, 2026

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

VIA ELECTRONIC MAIL

Re: Notification of Data Security Event

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents KDM Signs ("KDM") located at 10450 N Medallion Drive, Cincinnati, Ohio 45241, in connection with its response to a recent data event discussed below. The purpose of this letter is to notify you of the event in accordance with New Hampshire data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, KDM does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

1. Nature of the Security Event

On March 12, 2026, KDM experienced a network disruption. KDM promptly took steps to secure its network and initiated an investigation, with the assistance of cybersecurity experts, to determine what happened and whether any sensitive data may have been impacted. The investigation determined that an unknown actor entered our systems and acquired certain data on or about March 11, 2026. KDM then undertook a comprehensive review of the information involved and moved as quickly as possible to notify potentially impacted parties.

2. Number of Affected New Hampshire Residents & Information Involved

The event involved personal information for approximately 1 New Hampshire resident. The information involved in the event for New Hampshire resident included name and Social Security number.

3. Notification to Identified Individuals

On May 29, 2026, notification letters were sent to New Hampshire residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in complimentary identity protection services provided through TransUnion including 12 months of credit monitoring and identity theft services. A sample notification letter is enclosed.

4. Measures Taken to Address the Event

Upon identifying this event, in addition to taking the steps described above, KDM worked to learn more about what happened and what information could have been affected. KDM notified the identified individuals and provided them with steps they can take to protect their personal information, including providing them with information about its call center established to answer questions about the event, address related concerns, and assist with enrolling in the offered credit monitoring services. Further KDM is providing individuals with information on how to place a fraud alert and credit freeze on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

5. Contact Information

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

Sincerely,

Maria Efaplomatidis
Partner, Constangy Cyber Team

0001044

KDM Signs
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS3860

6_0001044 ##

kdm Powered by HirtsCarter

[redacted]

May 26, 2026

Subject: Notice of Data Security Incident

Dear [redacted]

KDM Signs ("KDM") is writing to inform you of a recent event that involved your personal information. KDM takes the privacy and security of information in our possession very seriously. We want to provide you with information about the event, steps we took in response, and steps you can take to guard against identity theft and fraud, including enrolling in credit monitoring and identity protection services at no cost to you.

What Happened. On March 12, 2026, KDM experienced a network disruption. KDM engaged independent cybersecurity specialists to investigate what occurred. The investigation determined that an unknown actor entered our systems and accessed certain data on or about March 11, 2026. We reviewed that data to determine whether it included any personal information. On May 13, 2026, our investigation confirmed that the reviewed data included some of your information. We then notified you of the event as quickly as possible.

What Information Was Involved. The reviewed data included your name and Social Security number.

What We Are Doing. As soon as we identified the disruption, we took the steps described above. We also implemented additional measures designed to reduce the risk of a similar event occurring in the future.

What You Can Do. We encourage you to follow the recommendations in this letter, which may help to protect your personal information. These recommendations include enrolling in the complimentary credit monitoring and identity protection services described below:

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must

enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. 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.

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 [redacted] Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern time, excluding holidays. Cyberscout representatives can help answer questions you may have regarding the event and the protection of your information.

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

Sincerely,

KDM Signs
10450 N Medallion Dr.
Cincinnati, OH 45241
(513) 769-3500

Additional Steps You Can Take To 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; monitoring free credit reports closely for errors; and 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 1-877-322-8228, 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 types 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 poof. 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 freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a freeze may interfere with or delay your ability to obtain credit. You must separately place a freeze on your credit file with each credit reporting agency. There is no fee to place or lift a freeze. For information and instructions on how to place a freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a 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 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. You cannot be charged to lift a freeze.

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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, credit/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.

Federal Trade Commission: The Federal Trade Commission can be reached at 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-438-4338; www.consumer.ftc.gov.

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; 1-202-727-3400; www.oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919;1-800-952-5225; http://oag.ca.gov/

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at:9001 Mail Service Center Raleigh, NC 27699-9001; 1-877-5-NO-SCAM (Toll-free within North Carolina);1-919-716-6000; 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; 1-212-416-8433; 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

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 1-800-621-0508; www.texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609;1-802-828-3171; www.ago.vermont.gov

Rhode Island: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI02903; 1-401-274-4400; or www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There is one Rhode Island resident that may be impacted by this event.