Kennedys

1600 Market St
Suite 1410
Philadelphia, PA 19103

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267.479.6706
Joshua.Mooney@kennedyslaw.com

December 15, 2025

Via E-Mail
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Breach

Dear Attorney General Formella:

Kennedys CMK, LLP represents Driven P.S.C., a Puerto Rico-based financial and accounting advisory firm. We write in accordance with the New Hampshire data breach notification statute, N.H. REV. STAT. § 359-C:20, requiring reporting to your office in the event of a data incident involving New Hampshire residents.[1]

On February 21, 2025, Driven became aware of suspicious sign-in activity related to single employee's email account. Driven retained our law firm and we retained the independent forensic firm Cypfer Inc. to assist our investigation for the rendering of legal advice. Our investigation determined that Driven suffered an unauthorized access to the employee's email account between February 3, 2025, and on February 21, 2025, as a result of a phishing event. We also learned that the account has been synced. On November 12, 2025, after conducting and validating the findings of a detailed review of all of the mailbox's contents, Driven confirmed that certain files in the account contained personal information and identified to whom that information belonged. On December 4, 2025, after receiving the results of a National-Change of Address review of the individuals identified, Driven confirmed that the information of one (1) New Hampshire resident was involved. The information included the individual's name and driver's license or state identification number.

Given the nature of its services, Driven was not the data owner for all of the data involved. Driven worked to identify the data owners associated with each individual for whose data Driven was acting as a service provider (or licensee), and it provided notification of the

[1] Respectfully, in making this submission, Driven does not waive its rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction over it.

Kennedys

incident to those data owners on December 3, 2025. As part of that notification, Driven is allowing the data owners to opt-in and authorize notification to be effectuated by Driven on their behalf.[2] Driven will proceed with a second wave of notification on behalf of the data owners once it obtains consent to notify the individuals.

Driven notified one (1) New Hampshire resident via First Class U.S. mail on December 12, 2025. The notified individual is offered the opportunity to activate complimentary identity monitoring services for twelve (12) months through TransUnion. A sample copy of the notification letter is enclosed. Driven places a strong emphasis on security awareness throughout the organization. This includes annual training for all employees. However, Driven is reviewing its existing security policies and protections already in place on its network and adopting additional security to safeguard against evolving threats moving forward. Multi-Factor Authentication (MFA) was enabled on the user's account. Along with maintaining MFA and ongoing employee security awareness training, Driven is configuring custom alerts in Microsoft Entra's sign-in monitoring to flag abnormal login locations or other unusual activity. Driven also continues to reinforce phishing awareness through regular training and internal communications.

If you have any questions or need additional information, please do not hesitate to contact me.

Very truly yours,

Joshua A. Mooney

Partner

for Kennedys

Enclosures: Sample Individual Notification Letter

[2] Notification is being effectuated in two waves. Individuals whose data Driven is the data owner were notified on December 12, 2025. This regulatory report is being filed in connection with this wave. A supplemental report will be provided after the second notification wave is completed if it involves personal information of residents of this state.

Driven
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

December 12, 2025

Re: ***Notice of Data Privacy Event***

Dear [redacted]:

Driven takes the privacy and security of your information seriously. As part of that commitment, we write to notify you of a data privacy event involving your personal information. This notice explains the incident, our response, and steps you can take to help protect your personal information, should you find it appropriate to do so. We are also offering complimentary credit monitoring and identity protection services.

What Happened: On February 21, 2025, we discovered suspicious sign-in activity related to an employee's email account. We took immediate action to secure the systems; this included engaging cyber incident response professionals to investigate the nature and scope of the incident. Through the investigation, we learned that data was taken from one user's email account by an unauthorized actor on February 21, 2025. On November 12, 2025, after conducting and validating the findings of a detailed review of the data set impacted, we confirmed that certain files contained personal information.

What Information Was Involved: Our review of the files determined your first and last name, in combination with your Social Security number were involved.

What We Are Doing: Upon learning of the incident, we took immediate steps to address it, including verifying and securing all of our email accounts. We engaged cyber incident response professionals, we reviewed our existing security policies and protections already in place on our network, and adopted additional security measures to safeguard against evolving threats moving forward.

As an added protection, we are offering Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (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.

What You Can Do: You should remain vigilant for incidents of identity theft and fraud, from any source, by reviewing your credit reports and account statements for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider. Please refer to the enclosed "*Steps You Can Take to Help Protect Your Information"* for additional resources to protect against fraud and identity theft, should you find it appropriate to do so.

000010103G0400

P

<u>For More Information:</u> Should you have any questions or concerns, please contact our dedicated assistance line with TransUnion at 1-800-405-6108 7:00 a.m. – 7:00 p.m. CST Monday through Friday, excluding major U.S. holidays. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Driven
Enclosure: *Steps You Can Take to Help Protect Your Information*

PO BOX [illegible]
San Juan Puerto Rico
[illegible]
[illegible]
www.[illegible].com

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Enrollment Instructions: 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.

Monitor Your Accounts and Credit Reports: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-378-4329 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information:

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For California Residents, the California Attorney General may be contacted at 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; and http://oag.ca.gov/.

For D.C. Residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.

For Maine Residents, the Maine Attorney General may be contacted at 6 State House Station, Augusta, ME 04333; 207-626-8800; and https://www.maine.gov/ag/.

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

For New York Residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina Residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon Residents, the Oregon Office of the Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; and www.doj.state.or.us.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. No Rhode Island resident's data was involved in this incident.

For Texas Residents, the Texas Attorney General may be contacted at 300 W. 15th Street, Austin, TX 78701; 800-621-0508; and texasattorneygeneral.gov/consumer-protection/.

For Vermont Residents, the Vermont Attorney General's Office may be contacted at 109 State Street, Montpelier, VT 05609; 802-828-3171; and ago.info@vermont.gov.

P 000010303O0000