



Sean B. Hoar, Partner & Chair
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
4800 Meadows Road, Suite 300
Lake Oswego, Oregon 97035
shoar@constangy.com
503.459.7707

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

June 26, 2026

VIA U.S. MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

RECEIVED
JUN 30 2026
CONSUMER PROTECTION

Re: Notice of Data Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Challenge Mfg. Company, LLC (“Challenge”) in connection with an incident described in greater detail below. Challenge is a supplier of complex assemblies and engineering metal formed products to the automotive industry and is headquartered in Grand Rapids, Michigan. Challenge is submitting this letter as a good faith effort to notify your office consistent with any reporting requirements Challenge may have under N.H. Rev. Stat. § 359-C:19-21. By providing this notice, Challenge does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data breach notification statute, or personal jurisdiction.

1. Nature of the Incident

On May 8, 2026, Challenge discovered unauthorized activity within its computer environment and immediately began investigating the incident. As part of its response, Challenge engaged third-party cybersecurity experts to assist with the process. On May 21, 2026, the investigation determined that certain files were acquired without authorization in connection with the incident. Challenge undertook a comprehensive review of those files to identify whether they contained any personal information and to whom that information pertained, as well as to locate address information to diligently notify affected individuals.

2. Number of Affected Residents

The information involved one (1) New Hampshire resident’s name and Social Security number. Challenge notified the resident on June 1, 2026 by USPS First Class Mail via the attached notification letter.

3. Steps Taken Relating to the Incident

Upon discovering the incident, Challenge took the steps referenced above. Challenge also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable. Challenge has also taken steps to improve the security of its network environment.

Challenge conducted a thorough review of the affected information, engaged a consumer remediation firm, and worked to notify individuals as soon as possible. As part of this process, Challenge arranged to provide the New Hampshire resident with complimentary identity protection services, including 12 months of credit monitoring, identity protection, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

4. Contact Information

Challenge takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please contact me at shoar@constangy.com or 503.459.7707 or Amanda Novak at anovak@constangy.com or 612.464.9113.

Sincerely,



Sean B. Hoar
Constangy, Brooks, Smith & Prophete, LLP

Encl. Sample Consumer Notice



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>>
 Enrollment Deadline: September 1, 2026
 To Enroll, Scan the QR Code Below:



SCAN ME

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

June 1, 2026

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

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

I am writing to inform you of a recent data security incident that may have affected your personal information. Challenge Mfg. Company, LLC (“Challenge”) takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On May 8, 2026, we discovered unauthorized activity in our computer environment and immediately began investigating the incident. We also engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain files were acquired without authorization. We undertook a comprehensive review of those files and, on or about May 21, 2026, learned that some of your personal information was contained within the affected data which is the reason for this notification.

What Information Was Involved. The information may have included your <<Variable Text 2: Affected Regulated Data Sets>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable. We are also offering complimentary identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit monitoring¹, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is September 1, 2026.

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 complimentary services offered to you through IDX by calling 1-844-889-7853, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

¹ 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.

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 1-844-889-7853 Monday through Friday from 9 am - 9 pm Eastern Time, excluding US holidays. 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,

Challenge Mfg. Company, LLC

Steps You Can Take to Help 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 (the "FTC").

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 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
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 Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
<https://consumer.ftc.gov>
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://oag.maryland.gov>
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
<https://ag.ny.gov>
800-771-7755

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212-416-8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
<https://oag.dc.gov/consumer-protection>
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
<https://ncdoj.gov/protectingconsumers/>
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.