Todd Rowe
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
20 North Wacker, Suite 4120
Chicago, IL 60606
trowe@constangy.com
773.558.2363

October 10, 2025

**VIA ELECTRONIC MAIL**
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

**Re: Notice of Data Security Incident**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP, represents Chalmers Insurance Group ("Chalmers") in connection with a recent data security incident. Chalmers takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of Chalmers pursuant to N.H. Rev. Stat. §§ 359-C:19-21 because personal information for 57 New Hampshire residents could have been involved in the data security incident.

## 1. Nature of the Security Incident

On April 13, 2025, Chalmers became aware of unusual activity involving its network systems. Chalmers engaged independent cybersecurity experts to assist with a comprehensive investigation of the activity. The investigation determined that certain files may have been acquired without authorization between April 8, 2025 and April 10, 2025. Chalmers thereafter undertook comprehensive review of all potentially affected emails to identify individuals whose information may have been involved and gather contact information needed to provide notice. This process concluded on September 8, 2025, at which time Chalmers arranged to provide notification.

The potentially affected personal information for New Hampshire residents included individuals' names, Social Security number, and/or driver's license or state identification.

## 2. Number of New Hampshire Residents Affected

Chalmers notified 57 New Hampshire residents within the potentially affected population whose personal information may have been involved on October 6, 2025, via USPS First-Class Mail. A sample copy of the notification letter sent to the potentially affected individuals is included with this correspondence.

## 3. Steps Taken Relating to the Incident



13579054v1

As soon as Chalmers discovered the unusual network activity, it took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been involved. Chalmers has also implemented security measures to further enhance its network security and reduce the likelihood of a similar incident occurring in the future

Chalmers has established a toll-free call center through Kroll to answer questions about the incident and address related concerns. Additionally, Chalmers is providing notified individuals with access to 12 months of free credit monitoring and identity protection services through Kroll.

**4. Contact Information**

If you have any questions or need additional information, please do not hesitate to contact me at 73.558.2363 or trowe@constangy.com.

Sincerely,

Todd Rowe
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter



13579054v1

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

Dear <<first_name>> <<last_name>>:

Chalmers Insurance Group ("Chalmers") is writing to inform you of a data security incident that may have affected your personal information. If you are not familiar with Chalmers, we work with companies, including <<b2b_text_1 (data owner)>>, to obtain insurance. We take the privacy and security of all information in our possession very seriously. This letter has information about the incident and steps you can take to help protect your information.

**What Happened.** On April 13, 2025, Chalmers became aware of unusual activity involving our network systems. We engaged independent cybersecurity experts to assist with a comprehensive investigation of the activity. The investigation determined that certain files may have been acquired without authorization between April 8, 2025 and April 10, 2025. As a result, we conducted a review of the potentially affected files and, in September 2025, learned that some of your information was contained within the potentially affected data. We then contacted <<b2b_text_1 (data owner)>> and worked with them to provide you this notice.

**What Information Was Involved**. The potentially affected information may have included your <<b2b_text_2 (Data Elements)>>.

**What We Are Doing.** As soon as Chalmers discovered the 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.

Additionally, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

**What You Can Do.** You can follow the best practices on the following page to help protect your information. We also encourage you to you activate your complimentary credit monitoring services using the enrollment code provided above.

**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 our dedicated team at (866) 291-2047 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays.

Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Chalmers Insurance Group
100 Main Street
Bridgton, ME 04009

## 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** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105851 | P.O. Box 9532 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19016 |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-916-8800 |
| www.equifax.com | www.experian.com | 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
consumer.ftc.gov
877-438-4338

**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.

KROLL

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit 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.

### $1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.