MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

RECEIVED
APR 24 2023
CONSUMER PROTECTION

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 19, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

To Whom it May Concern:

We represent Conner Strong & Buckelew Companies, LLC ("CSB") located at 2 Cooper Street, Camden, New Jersey 08102, and are writing to notify your Office of an incident that may affect the security of certain information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CSB 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.

Nature of the Data Event

CSB identified suspicious activity related to an employee's email account. CSB immediately took steps to secure the account and launched an investigation with the assistance of third-party forensic investigators to determine the nature and scope of the activity. The investigation determined that email accounts belonging to certain CSB employees were subject to unauthorized access on separate occasions between February 7, 2022 and March 30, 2022. While the investigation confirmed the accounts were subject to unauthorized access, it was unable to identify all emails or attachments within the accounts that the unauthorized individual may have accessed or acquired.

Therefore, out of an abundance of caution, CSB, with the assistance of third-party forensic investigators, conducted a programmatic and manual review of the entire contents of the email accounts for emails or attachments that contained protected information at the time of this activity and to which individuals the information relates. Once complete, CSB then began an extensive review of its internal files in order to determine which clients the information belonged and address information in order to provide them with notice of the event. Following the review, on or about January 24, 2023, CSB began notifying potentially impacted clients of this incident, because certain current and/or former employees and their beneficiaries were identified during the review. While the information varies by individual, the impacted information includes . Based on the ongoing

investigation, notice, and response, CSB received address information from clients and is providing notice to impacted individuals and regulators, as required, on its clients' behalf.

Notice to New Hampshire Resident

On or about April 18, 2023, CSB mailed written notice of this incident to affected individuals, which includes one (1) New Hampshire resident on behalf of the impacted clients. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification to impacted clients and individuals is ongoing, and CSB may supplement this notification if it determines that a significant amount of additional New Hampshire residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, CSB moved quickly to investigate and respond to the incident, assess the security of CSB systems, and identify potentially affected individuals and CSB clients. CSB immediately reset the email account passwords, confirmed the security of relevant systems, reviewed policies and procedures, and implemented additional security measures and training to its employees.

CSB is providing access to complimentary credit monitoring services for one (1) year, through Experian to individuals whose Social Security number or driver's license information was potentially affected by this incident. Additionally, CSB is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/klh
Enclosure

EXHIBIT A

CONNER
STRONG &
BUCKELEW

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_5 (CA variable header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Conner Strong & Buckelew ("CSB") is writing to inform you of a recent incident that may impact the security of some of your information. CSB received your information as part of the normal course of business providing insurance and brokerage consulting services to <<b2b_text_1 (data owner)>>.While we are unaware of any actual or attempted misuse of your information, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft or fraud, should you feel it necessary to do so.

What Happened? CSB discovered suspicious activity related to certain CSB employee email accounts. Upon discovering this activity, we immediately took steps to secure the accounts and launched an investigation with the assistance of third-party forensic investigators to determine the nature and scope of the event. The investigation determined that email accounts belonging to certain CSB employees were subject to unauthorized access on separate occasions between February 7, 2022 and March 30, 2022. As a result, the unauthorized actor may have had access to certain emails and attachments within these accounts.

What Information Was Involved? The investigation was unable to identify all emails or attachments in the accounts that the unauthorized individual may have accessed or acquired. Therefore, out of an abundance of caution, we conducted a review of the entire contents of the email accounts for emails or attachments that contain personal information and CSB notified <<b2b_text_1 (data owner)>> of this incident. This review was recently completed and we are notifying you of this incident because the investigation confirmed that your information was present at the time of the incident. The impacted information that is related to you includes your <<b2b_text_2 (data elements)>><<b2b_text_3 (data elements cont.)>>. To date, CSB is not aware of any actual or attempted misuse of your information.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. When we discovered this incident, we immediately reset the impacted email account passwords and took steps to determine what information was in the impacted accounts and to which CSB clients the information belonged. We further confirmed the security of our employee email accounts and related systems and are reviewing and strengthening our existing policies, procedures, and safeguards related to cybersecurity. We have also notified appropriate state and federal regulators.

As an added precaution, we are offering you complimentary access to 12 months of credit and identity monitoring, fraud consultation, and identity theft restoration services through Experian. We encourage you to enroll in these services, as we are not able to enroll you on your behalf. More information and instructions on how to enroll in these services may be found in the attached *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at xxx-xxx-xxxx, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Conner Strong & Buckelew

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<b2b_text_6 (activation date)>> no later than 5:59 pm CT (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit**
- Provide your **activation code**: <<Activation Code s_n>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by <<b2b_text_6 (activation date)>>. Be prepared to provide engagement number <<b2b_text_4 (engagement #)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.marylandattorneygeneral.gov. CSB is located at 2 Cooper St. Camden, NJ 08102.

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.

NH DEPT OF JUSTICE
APR 24 '23 PM2:38