



Simone McCormick
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Simone.McCormick@lewisbrisbois.com
Direct: 971.334.7010

August 20, 2019

File No. 39395.181

VIA E-MAIL

Attorney General Gordon MacDonald
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 Security Incident**

Dear Attorney General MacDonald:

We represent Cornerstone, Inc. ("Cornerstone"), located in Eau Claire, Wisconsin, in connection with a recent data security incident described below.

1. Nature of the data security incident.

On or around July 9, 2019, Cornerstone learned that an unauthorized third party may have obtained a Cornerstone applicant's online rental application, which contained that individual's personal information. With the assistance of its IT provider, Cornerstone immediately began an investigation to determine how the applicant's information may have been compromised, and if any personal information was accessed or acquired without authorization. Based on its investigation, Cornerstone determined an unauthorized actor may have gained access to the database which stores rental applications on or about June 26–28, 2019.

Following this discovery, Cornerstone extensively reviewed the database's contents to determine which individuals' information may have been affected by any potential unauthorized access, in order to inform all potentially affected individuals of the incident.

It appears the following types of information may have been impacted by this incident: names, addresses, Social Security numbers, dates of birth, driver's license information, and/or telephone numbers.

2. Number of New Hampshire residents affected.

With the assistance of counsel, Cornerstone completed a final notification list of potentially affected individuals on August 12, 2019, and engaged an outside notification vendor to facilitate the notification process.

Cornerstone ultimately identified two (2) New Hampshire residents whose information may have been impacted by this incident. Notification letters were mailed to all potentially impacted individuals with valid address information on August 19, 2019. A sample copy of the letter provided to potentially impacted individuals is included with this letter.

3. Steps taken relating to the incident.

Cornerstone has taken measures to further enhance the security of personal information in its possession and to prevent similar incidents from happening in the future, including the steps described above. Cornerstone also disabled its online rental application process and it is resetting user credentials. In addition, Cornerstone has notified the FBI about this incident, and will work with and provide assistance to law enforcement to hold the perpetrators accountable.

Cornerstone is also offering notified individuals complimentary credit monitoring and identity protection services for one year through TransUnion.

4. Contact information.

Please contact me at 971.334.7010 or by email at Simone.McCormick@lewisbrisbois.com if you have any questions.

Sincerely,

Simone McCormick of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SM:BMT
Encl.: Consumer Notification Letter



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Subject: Notice of Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a data security incident that may have involved a rental application that was previously submitted to Cornerstone, Inc. (“Cornerstone”) which listed you as a potential tenant and contained some of your personal information.

The privacy and security of your personal information is extremely important to us. That is why we are writing to inform you about this incident, offer you complimentary credit monitoring and identity protection services, and provide you with information relating to steps that can be taken to help protect your information.

What Happened? On or around July 9, 2019, Cornerstone learned that an unauthorized third party may have obtained a Cornerstone applicant’s online rental application, which contained that individual’s personal information. With the assistance of its IT provider, Cornerstone immediately began an investigation to determine how the applicant’s information may have been compromised, and if any personal information was accessed or acquired without authorization. Based on its investigation, Cornerstone cannot rule out that an unauthorized actor may have gained access to the database which stores rental applications on or about June 26–28, 2019. Therefore, Cornerstone determined which individuals’ information may have been affected by any potential unauthorized access to the database in order to inform all potentially affected individuals of the incident.

Because of the nature of the information, we are writing to inform you of the incident out of an abundance of caution and to provide you with access to complimentary credit monitoring and identity protection services.

What Information Was Involved? The types of information that may have been impacted include: names, addresses, Social Security numbers, dates of birth, driver’s license information and telephone numbers.

What Are We Doing? As soon as Cornerstone discovered the incident, we took the steps described above. We have also taken measures to further enhance the security of personal information in our possession and to prevent similar incidents from happening in the future, including disabling our online rental application process and resetting user credentials. In addition, we have notified the Federal Bureau of Investigation (“FBI”) about this incident, and we will work with and provide assistance to law enforcement to hold the perpetrators accountable.

We are also providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering you complimentary credit monitoring and identity protection services for one year through TransUnion®, one of the three nationwide credit reporting companies.

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<**12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<**PassCode**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Date**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What You Can Do: You can follow the recommendations on the following page to protect your personal information. We recommend that you review your credit report and consider placing a security freeze on your credit file.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions concerning this incident, please contact 855-683-4611, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Doug Ottum
Cornerstone, Inc.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 <http://www.annualcreditreport.com/>, calling toll-free 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 also 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
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.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 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. 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>.

Security Freeze: Under U.S. law, 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

**Maryland Attorney
General**

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island
Attorney General**

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.