



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

May 10, 2021

VIA WEB PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, Maine 04330
E-Mail: breach.security@maine.gov

Re: **Notification of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents C.E. Floyd Company ("C.E. Floyd"), a general contractor and construction manager with offices in Connecticut and Massachusetts, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute.

1. Nature of the Incident

On April 8, 2021, a company employed by C.E. Floyd to securely dispose of sensitive paper records inadvertently released records belonging thereto. Upon learning of this inadvertent release of paper records, C.E. Floyd took immediate steps to recover the records that had been inadvertently released in order to minimize the potential exposure of information contained therein. C.E. Floyd then reported this matter to law enforcement and conducted an investigation to determine what data may have been impacted. C.E. Floyd Company determined that the inadvertently released records may have contained personal information belonging to certain Maine residents.

Although C.E. Floyd has no evidence of access to, acquisition of, or misuse of any information contained within the inadvertently released paper records, C.E. Floyd provided notification of this incident out of an abundance of caution.

2. Type of Information and Number of Maine Residents Involved

As a result of C.E. Floyd's investigation, C.E. Floyd determined that the incident may have impacted

personal information belonging to one Maine resident. The potentially impacted information may have included name, Social Security number, driver's license number, financial account information, and/or payment card information.

Potentially impacted individuals identified as a result of the C.E. Floyd investigation were mailed a letter notifying them of the incident, offering complimentary identity theft protection services, and providing information regarding additional steps that they can take to help protect their personal information. The notification letters were sent via USPS First Class Mail on May 11, 2021.

3. Measures Taken to Address the Incident

Upon learning of this incident, C.E. Floyd took steps to recover and securely dispose of the paper records that were inadvertently released and launched an investigation to identify potentially impacted individuals/information. C.E. Floyd also reported this incident to law enforcement and will cooperate fully with any law enforcement investigation relating thereto.

Additionally, C.E. Floyd has notified the potentially impacted individuals and provided them with information about steps that they can take to help protect their personal information as well as complimentary credit monitoring, dark web monitoring, identity theft insurance, and fully managed identity theft restoration services.

4. Contact Information

C.E. Floyd remains dedicated to protecting all information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052 or Alyssa.Watzman@lewisbrisbois.com.

Sincerely,



Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

ARW:vhv

Enclosure: Sample Consumer Notification Letter



C.E. Floyd Company, Inc.

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

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

<<Date>>

Re: Notification of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a recent data security incident experienced by C.E. Floyd Company that may have involved your personal information. Please read this letter carefully as it contains information regarding the incident, the type of personal information potentially impacted, and steps that you can take to help protect your personal information.

What Happened: On April 8, 2021, a company employed by C.E. Floyd Company to securely dispose of confidential paper records inadvertently released records belonging thereto. Upon learning of this inadvertent release of records, C.E. Floyd Company took immediate steps to recover the records that had been inadvertently released in order to minimize the potential exposure of information contained therein. C.E. Floyd Company then reported this matter to law enforcement and conducted an investigation to determine what data may have been impacted. That same day, C.E. Floyd Company determined that the inadvertently released records may have contained personal information belonging to certain former employees as well as designated beneficiaries thereof. Out of an abundance of caution, C.E. Floyd Company then worked diligently to identify address information associated with such individuals in order to provide notification of this incident. Importantly, C.E. Floyd Company is not aware of any misuse of your personal information as a result of this incident.

What Information Was Involved: The information impacted in connection with this incident may have included your name, Social Security number, driver's license number, financial account information, and / or payment card information.

What We Are Doing: Upon learning of this incident, C.E. Floyd Company took the steps described above. Specifically, C.E. Floyd Company took steps to recover and securely dispose of the records that were inadvertently released and launched an investigation to identify potentially impacted individuals / information. C.E. Floyd Company also reported this incident to law enforcement and will cooperate fully with any law enforcement investigation relating thereto.

C.E. Floyd Company is now providing you with information about steps that you can take to help protect your personal information. Furthermore, even though C.E. Floyd Company has no evidence of misuse of your personal information as a result of this incident, as an added precaution, we are offering complimentary identity theft protection services through TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. These services include 12 months of credit monitoring and dark web monitoring, \$1,000,000 in identity theft insurance with no deductible, and fully managed identity theft recovery services. To receive the identity theft protection services, you must enroll by <<date>>.

What You Can Do: We encourage you to enroll in the complimentary identity theft protection services by going to **www.MyTrueIdentity.com** and following the instructions provided. When prompted, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your services. We also recommend that you review the information on the following page for additional steps to help protect your personal information, which include placing a fraud alert on your credit report and 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 call C.E. Floyd Company at 781-271-9006 ext. 110.

The security of all information is a top priority for C.E. Floyd Company. We are committed to safeguarding your data and privacy.

Sincerely,

A handwritten signature in blue ink that reads "Christopher J. Floyd". The signature is written in a cursive, flowing style.

Christopher J. Floyd, President / CEO
C.E. Floyd Company

Steps You Can Take to Further Protect Your Information

Review Your Account Statements for Suspicious Activity: We recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect suspicious activity, promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraud or suspected identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Credit Reports: 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 annualcreditreport.com, calling toll-free 877-322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. The request form is available at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. 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 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors 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. Additional information is available at 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 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, 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. 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, address history, 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 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, 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

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

Your 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 others. For more information about the FCRA and your rights, please visit: http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>.