

DECOTIIS

DeCotiis, FitzPatrick, Cole & Giblin, LLP

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>>

Dear <<Name 1>>:

DeCotiis, FitzPatrick, Cole & Giblin, LLP (“DFCG”) is writing to inform you of a recent incident that may impact the security of some of your personal information. DFCG received your information in the course of a legal matter in which you were either directly or indirectly involved as a party. While we are unaware of any actual or attempted misuse of your personal 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 and fraud, should you feel it is necessary to do so.

What Happened? On or about May 4, 2020, DFCG learned of suspicious activity related to a DFCG employee email account. Upon learning of this activity, we immediately took steps to secure the account and began an investigation, which included working with third-party IT experts and forensic investigators, to determine the nature and scope of the activity. Through this investigation we determined that an unknown actor gained unauthorized access to certain DFCG employee email accounts for a limited timeframe on separate occasions between April 28, 2020 and May 8, 2020. During this limited timeframe, the unauthorized actor may have had access to certain emails and attachments within the accounts.

What Information Was Involved? While the investigation was able to determine certain email accounts were accessed, it was unable to determine whether any specific email or attachment was actually accessed by the unauthorized actor. Therefore, in an abundance of caution, on or about September 16, 2020, DFCG, with the assistance of third-party forensic investigators, completed an extensive, programmatic and manual review of the contents of the impacted email accounts to determine the types of protected or confidential information contained in the email accounts and to which individuals the information relates. Upon completion of this review, DFCG immediately launched a review of its files to ascertain address information for the impacted individuals. Our review confirmed that your <<Breached Elements>> were present in one of the email accounts at the time of this incident. To date, DFCG has not received any reports of 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 relevant account passwords and took steps to determine what personal, sensitive, and confidential data was at risk. We also confirmed the security of our employee email accounts and related systems. As part of our ongoing commitment to the security of personal information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security. We will also be notifying state regulators, as required.

As an added precaution, we are also offering you complimentary access to twelve (12) months of credit and identity monitoring, fraud consultation and identity theft restoration services through TransUnion. We encourage you to activate these services, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. You may review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also activate the complimentary credit and identity monitoring services we are offering.

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 DFCG at our dedicated assistance line at 800-409-9485, Monday through Friday, between the hours of 9 am to 9 pm Eastern Time. You may also write to DFCG at 61 S. Paramus Road, Suite 250, Paramus, New Jersey 07652.

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

Sincerely,

A handwritten signature in black ink, appearing to read 'J. DeCotiis', with a long horizontal flourish extending to the right.

Joseph M. DeCotiis
DeCotiis, FitzPatrick, Cole & Giblin, LLP



STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit and Identity Monitoring

Activation Code: <<Activation Code>>

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

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

How to Enroll: You can sign up online or via U.S. mail delivery

- 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 12-letter Activation Code <<Insert Unique 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 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 six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> 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 Deadline>>. 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 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.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- 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 credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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, military identification, 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 fraud alert or 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
888-298-0045	1-888-397-3742	833-395-6938
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 Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here.

Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are **XX** Rhode Island residents impacted by this incident.