



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

MAR 04 2021

CONSUMER PROTECTION

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

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

February 25, 2021

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

Dear Sir or Madam:

We represent Federal Contractors, Inc. ("FCI") located at 623 Underwood Street, NW, Washington, DC 20012, and are writing to notify your office of an incident that may affect the security of some personal information relating to 1 New Hampshire resident. This notice may be supplemented with any significant facts learned subsequent to its submission. By providing this notice, FCI 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

FCI became aware of unusual activity related to an employee's email account and immediately took steps to change the user's password and commenced an investigation to determine the nature and scope of the incident with assistance from third-party computer forensic specialists. On September 8, 2020, the investigation determined that an unauthorized actor(s) gained access to an FCI employee email account at various times between June 1 and June 25, 2020.

The contents of the impacted email account were next reviewed through a time-consuming manual and programmatic process to determine what sensitive data may have been accessible. FCI confirmed the identities of the individuals who may have had information accessible as a result of the incident and launched an exhaustive review of internal files to ascertain address information for the impacted individuals. Although FCI is unaware of any actual or attempted misuse of any information, FCI is notifying potentially affected individuals out of an abundance of caution.

The information that could have been impacted includes name, address and Social Security number.

Notice to New Hampshire Resident

On or about February 24, 2021, FCI provided written notice of this incident to all affected individuals, which includes 1 New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

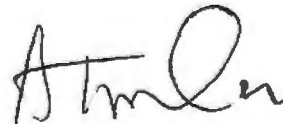
Upon discovering the event, FCI moved quickly to investigate and respond to the incident, assess the security of FCI systems, and notify potentially affected individuals. FCI is also working to implement additional safeguards and training to its employees. FCI is providing access to credit monitoring services for two (2) years through IDX to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FCI is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FCI is providing individuals with 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 (267) 930-4801.

Very truly yours,



Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/msf

EXHIBIT A

[Federal Contractors Letterhead]

[Date]

[Individual Name]

[Address]

[City], [State] [Zip Code]

Dear [Name]:

Federal Contractors, Inc. (“FCI”) writes to inform you of a recent event that may affect the security of some of your personal information. While, to date, we have no evidence that your information has been misused, we are making you aware of the event, so you may take steps to better protect your information, should you feel it appropriate to do so.

What Happened. FCI became aware of unusual activity related to an employee’s email account. FCI immediately took steps to change the user’s password and commenced an investigation to determine the nature and scope of the incident with assistance from third-party computer forensic specialists. On September 8, 2020, the investigation determined that an unauthorized actor(s) gained access to an FCI employee email account at various times between June 1 and June 25, 2020.

The contents of the impacted email account were next reviewed through a time-consuming manual and programmatic process to determine what sensitive data may have been accessible. We confirmed the identities of the individuals who may have had information accessible as a result of the incident and launched an exhaustive review of our files to ascertain address information for the impacted individuals. Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because your information was present in the impacted email account.

What Information Was Involved. Our investigation determined that the following information related to you was present in the email account at the time of the incident: {data elements}, and name.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of unusual activity in an employee email account, we immediately commenced an investigation to confirm the nature and scope of the event and identify what personal information may have been present in the affected emails. With the assistance of third-party forensic investigators, we have been working to identify and put in place resources to assist potentially affected individuals. While we have stringent security measures in place to protect information in our care, we are implementing additional safeguards to further protect the security of information in our systems, including the implementation of multi-factor authentication for all employee email accounts. We will also be reporting this incident to state regulators, as appropriate.

As an added precaution, we are offering you access to identity theft protection services through IDX. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The cost of these services will be paid for by FCI. More information on these services, as well as instructions about how to enroll, may be found in the enclosed “Steps You Can Take To Help Protect Your Information.” Please note that you must complete the enrollment process, as we are not able to enroll you in these services on your behalf.

What You Can Do. We encourage you to review the enclosed “Steps You Can Take to Help Protect Your Information.” You may also enroll in free IDX identity protection services by going to <https://app.idx.us/account-creation/protect> or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is June 6, 2021.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at (202) 232-2068 .

Again, FCI takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Lisa Deane

Lisa Deane
Federal Contractors, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION



Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> or call 1-800-939-4170 and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is June 6, 2021.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

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 you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.htm	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338). 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.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023 (within Maryland) or 1-410-576-6300.

Washington D.C. Residents: the Office of Attorney General for the District of Columbia can be reached at: 441 4thStreet NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.