Maria Efaplomatidis, Partner
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
mefaplomatidis@constangy.com
Direct: 718-719-6475

March 20, 2024

VIA ONLINE SUBMISSION
Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Security Incident

Dear Attorney General Ferguson:

We represent Axiom Construction and Consulting, LLC ("Axiom"), a construction company focusing on architectural sheet metal headquartered in Washington, in connection with a recent data security incident, described in greater detail below. Axiom takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of Axiom because personal information for Washington residents could have been involved in the data security incident.

Nature of the Security Incident

On October 30, 2023, Axiom identified potential unauthorized activity resulting in a network disruption. In response, Axiom immediately took steps to secure the digital environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive or personal information may have been accessed or acquired during the incident. The investigation concluded on January 22, 2024 and identified that personal information belonging to certain employees may have been accessed or acquired without authorization. Following this determination, Axiom conducted a thorough review to verify the types of personal information involved and the names and contact information for all potentially impacted individuals to effectuate notice. This process was completed on March 15, 2024.

The personal information varied for potentially affected individuals but may have included name, date of birth, and Social Security number.

Number of Washington Residents Affected

Axiom notified 1,127 Washington residents within the potentially affected population on March 20, 2024, via USPS First-Class Mail. The attached notification letter is a template of what was provided to impacted individuals, or a substantially similar version thereof.

Steps Taken Relating to the Incident

Upon discovering this incident, in addition to taking the steps described above, Axiom took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. Axiom has taken immediate steps to evaluate and improve the security of its systems and will continue to evaluate additional protections that can be put into place to supplement its existing security policies and procedures.

In addition, Axiom is offering 12 months of complimentary credit and identity monitoring services to the potentially affected individuals through Kroll.

Contact Information

If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Maria Efaplomatidis
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter

AXIOM

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

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

Subject: Notice of Data Security Incident

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

I am writing to inform you of a recent potential data security incident at Axiom Construction & Consulting, LLC ("Axiom") that may have affected your personal information. Axiom takes the privacy and security of personal information very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened? On October 30, 2023, Axiom became aware of a network incident that affected our computer systems. Upon discovering this activity, we took immediate steps to secure the environment and engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened. This investigation remains ongoing. While we continue to investigate the incident and while we do not have evidence that employee data was misused, we are offering employees and former employees complimentary identity protection and credit monitoring out of an abundance of caution.

What Information Was Involved? The potentially affected information included your <<b2b_text_1 (Data Elements)>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. In addition, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do: We recommend that you review and implement the guidance included with this letter about how to help protect your information. We also encourage you to activate the services offered to you through Kroll.

For more information. Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call TFN, Monday through Friday from 8am – 5:30pm Central Time, excluding major U.S. holidays. Please have your membership number ready.

We take the privacy and security of all information within our possession very seriously. Please accept our sincere apologies and know that Axiom deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Megan Kalma
General Manager
1841 Front Street
Lynden, WA 98264

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing 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 also should 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 (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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	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 one year. 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: 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.

Federal Trade Commission	**Maryland Attorney General**	**New York Attorney General**
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 1-212-416-8433

North Carolina Attorney General	**Rhode Island Attorney General**	**Washington D.C. Attorney General**
9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 1-401-274-4400	441 4th Street, NW Washington, DC 20001 oag.dc.gov 1-202-727-3400

You also have certain 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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.