



Richard Goldberg, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19103
rgoldberg@constangy.com

February 21, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents GC Services in connection with a data security incident, which is described in greater detail below.

1. Nature of Incident

On January 16, 2024, we learned that at least one resident of Maine may have had their personal information involved in our client’s data security incident. The incident began on September 11, 2023, when the company experienced a computer outage that disrupted access to certain local cyber systems. After detecting and promptly containing the incident, the company launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident. Through that investigation, the company learned that someone may have gained unauthorized access to its network between and potentially acquired certain files, some of which contained personal information.

The potentially impacted information included individual’s name, address, social security number, account number, and routing number.

2. Number of residents affected

The company is notifying residents of the incident via first class U.S. mail on February 14, 2024. We expect the number of involved residents to be 13. The notification letter will describe the incident, information potentially involved, actions taken, protection available to residents (including credit monitoring), and provide contact and help information.

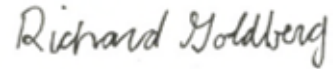
3. Steps taken relating to the incident

As soon as GC Services discovered the incident, it took the steps described above. In addition, GC Services notified law enforcement and will notify the potentially involved person shortly. To reduce the likelihood of a similar incident occurring in the future, the company took steps to further bolster the security of its network. Lastly, GC Services is offering notified individuals complimentary credit monitoring and identity protection services.

4. Contact information

GC Services takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 917.744.1760 or rgoldberg@constangy.com.

Sincerely yours,

A handwritten signature in cursive script that reads "Richard Goldberg".

Richard Goldberg of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Consumer Notification Letter



Return to IDX
4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

<< First Name>> <<Middle Name>> << Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

January 30, 2024

Subject: Notice of Data Security <<Breach/Incident >>

Dear << First Name>> <<Middle Name>> << Last Name>> <<Suffix>>:

The purpose of this communication is to notify you of a data security incident experienced by GC Services. We provide collection services for various clients, including financial institutions. This incident may have involved data used by us to help provide those services. Of course, we prioritize maintaining the privacy and security of all information in our possession. That is why we are notifying you of the event and providing you with resources to help protect your information.

What Happened: On January 16, 2024, we learned that your personal information may have been involved in a data security incident. On September 11, 2023, we experienced a computer outage that disrupted access to certain local cyber systems. After detecting and promptly containing the incident, we launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident. Through that investigation, we learned someone may have gained unauthorized access to our network between September 11 and September 20, 2023 and potentially acquired certain files, some of which contained personal information. We then researched whose information may have been involved and learned that your personal information may have been involved. Intelogix then took steps to notify people whose information may have been involved.

What Information Was Involved? The information involved in this incident may have included your name, <<Variable Text 2: data elements>>.

What We Are Doing: Upon discovering this incident, we launched an investigation and took steps to secure our network. We took steps to help prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and will continue to offer assistance in their investigation.

We are also offering you access to credit monitoring and identity theft protection services through IDX, A ZeroFox Company – a data breach and recovery services expert. These services include: <<12/24>> months of credit and dark web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll, please call (888) 618-5531 or visit <https://app.idx.us/account-creation/protect>. The enrollment code is <<Code>>. Please note that the deadline to enroll is April 30, 2024.

What You Can Do: We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact (888) 618-5531, Monday through Friday from 8:00 am – 8:00 pm Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

We regret any worry or inconvenience that this may cause you.

Very truly yours,

GC Services
6330 Gulfton St.
Houston, Texas 77081
713-776-6485

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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

P.O. Box 105851
Atlanta, GA 30348
1 (888) 378-4329
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 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

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

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>.

