



Lauren Godfrey, Esq.
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
322 North Shore Dr.
Building 1B, Suite 200
Pittsburgh, PA 15212
503.312.6251
lgodfrey@constangy.com

August 2, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Department of Professional and Financial Regulation
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Attorney General Anthony G. Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Basement Systems, Inc. (“Basement Systems”), located in Connecticut, in connection with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On May 13, 2024, Basement Systems became aware of unusual network activity and immediately took steps to secure its systems. Basement Systems also engaged cybersecurity experts to conduct an investigation to determine the scope of potential unauthorized activity and whether any sensitive or personal information may have been accessed or acquired. That investigation identified that certain data may have been acquired without authorization as a result of the incident. Following this discovery, Basement Systems undertook a preliminary review of the information that may have been involved in the incident. On July 3, 2024, Basement Systems identified that a limited amount of employee personal information was contained in the data. Since that time, Basement Systems has been working to gather contact information needed to provide notice to potentially affected individuals.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately two (2) Maryland residents. The information involved in the incident for the affected Maryland residents may have included name and Social Security number.

3. Notification to Affected Individual(s)

On August 1, 2024, notification letters were sent to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers individuals the opportunity to enroll in 24 months of complimentary identity protection services, including credit monitoring, and identity remediation services, as well as access to a call center, should any individual have questions about the incident. A sample notification letter sent to the impacted individual(s) is included with this correspondence.

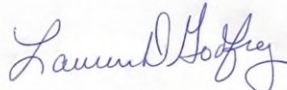
4. Steps Taken Relating to the Incident

Basement Systems is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above. Basement Systems has also established a toll-free call center through TransUnion, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, Basement Systems has also notified law enforcement, implemented new technical safeguards, strengthened security, and revised policies and procedures.

5. Contact Information

Basement Systems remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

A handwritten signature in blue ink that reads "Lauren Godfrey". The signature is fluid and cursive, with the first name "Lauren" and last name "Godfrey" clearly distinguishable.

Lauren Godfrey

Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter

Basement Systems, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



<<First Name>> <<Last Name>>
<<Address 1 / Address2>>
<<City>>, <<State>> <<Zip>>



August 1, 2024

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

Dear <<First Name>> <<Last Name>>:

Basement Systems, Inc. ("Basement Systems") is writing to notify you of a recent incident that may have affected your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened? On May 13, 2024, Basement Systems discovered that it had experienced an incident that temporarily disrupted the operability of our computer network. Upon discovery, Basement Systems promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. In addition, Basement Systems began working to restore impacted systems as quickly as possible. Basement Systems engaged a nationally-recognized digital forensics firm to conduct an independent investigation into what happened and determine whether personal information was accessed or acquired without authorization. The investigation determined that an unauthorized individual may have accessed data on our network between April 12, 2024 and May 14, 2024. On July 3, 2024, we learned that your information may have been involved.

What Information was Involved? The information may have included your name and Social Security number.

What Are We Doing? As soon as Basement Systems discovered the incident, we took the actions described above as well as implementing aggressive measures to enhance network security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

In addition, Basement Systems is providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.

Was your information misused? Receiving a letter does not mean that your information has been or will be misused. At this time, Basement Systems does not have evidence that your information was misused.

What You Can Do. We recommend that you review the *Steps You Can Take to Help Protect Your Information* included with this letter for guidance on how you can protect your information, and take advantage of the complimentary services offered to you through TransUnion. TransUnion will work on your behalf to help resolve issues you may experience as a result of this incident.

For More Information: If you have questions about this letter or need assistance, please do not hesitate to reach out to our designated call center at Cyberscout at 1-800-405-6108, Monday through Friday from 8 AM to 8 PM Eastern Time, excluding holidays and they will be happy to provide you with additional information.

We take your trust in us very seriously and thank you for your understanding in this matter.

Sincerely,

A handwritten signature in dark ink, appearing to be 'RC' or 'Richard Cleri', written in a cursive style.

Richard Cleri
Chief Marketing Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit monitoring: To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<code>>.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords.

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report and obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is listed below:

- **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.
- **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

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 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 can print this form 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 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report--an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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 the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.