Robert Bender
Constangy, Brooks, Smith & Prophete, LLP
bbender@constangy.com
445.308.1588
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

June 26, 2025

VIA ONLINE SUBMISSION

Re: Notification of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Calton & Associates, located at 2701 N. Rocky Point Drive, Suite 1000, Tampa, Florida 33607 in conjunction with their response to a recent data event involving information for Washington residents. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute. Calton & Associates does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the data breach notification statute, or personal jurisdiction.

1. Nature of the Security Incident

In late March 2025, Calton & Associates identified a network disruption. Calton & Associates immediately investigated with assistance from cybersecurity experts. The investigation determined unauthorized individuals accessed the network on March 28, 2025 and accessed some files on the network during that window. Calton & Associates undertook a comprehensive review of those files to determine the specific information present in the files. After completing the review and identifying the individuals whose information was in the files, Calton & Associates confirmed available address information so it could notify these individuals. That process was completed on June 20, 2025.

2. Number of Affected Washington Residents & Information Involved

The incident involved information for approximately 662 Washington residents. The information involved in the incident for Washington residents include names, addresses, Social Security numbers, and account numbers.

3. Notification to Affected Individuals

On June 26, 2025, Calton & Associates notified Washington 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 the opportunity to enroll in complimentary identity protection services including 12 months of credit monitoring, dark web monitoring, $1 million identity fraud

loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

Upon discovering this incident, Calton & Associates conducted an immediate and comprehensive investigation to confirm the scope of the event to secure its network and to notify affected individuals. Calton & Associates immediately reported the event to the FBI and FINRA and also notified the Federal Trade Commission. Calton & Associates established a toll-free call center through TransUnion to answer questions about the incident and to address related concerns. Calton & Associates continues to review policies and procedures and so it can implement additional measures as appropriate.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at bbender@constangy.com or 445-308-1588.

Sincerely,

Robert H. Bender

Robert Bender
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter

Calton & Associates
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

June 26, 2025

Subject: Notice of Data Security Incident

Dear [redacted]

At Calton & Associates, your trust is our highest priority, and we are deeply committed to safeguarding the privacy and security of your personal information. We are writing to inform you of a recent data security incident that involved your personal information, and to assure you that we have taken swift, decisive action to address it. This letter provides details about the incident, the robust steps we are taking to protect you, and resources available to help protect your personal information, giving you peace of mind.

What Happened. On April 25, 2025, we determined some of your information was involved in the subject incident. The incident and our response efforts began on March 28, 2025, when we experienced a network disruption and started investigating immediately, with support from cybersecurity. From the investigation, we determined unauthorized individuals accessed our network on March 28, 2025 and took certain files during this window. We conducted a meticulous review of those files to determine what information was accessible to the unauthorized individuals and discovered some of your personal information was contained within the potentially affected data which is the reason for this notification. Please rest assured that throughout our investigation, review, and mitigation, your best interest was our top priority.

What Information Was Involved. The information may have included your Name, address, social security number, and account number. Please note that we have no evidence of any misuse, or attempted misuse, of any information due to the incident. The security of your information remains our top concern, and we are taking every precaution to ensure it stays that way.

What We Are Doing. Upon identifying the incident, we took immediate steps to ensure the unauthorized individuals no longer had access to our network. Furthermore, to enhance network security and to minimize the risk of a similar incident occurring in the future, we implemented additional cybersecurity measures. We reported the event to the FBI and are fully cooperating with their investigation. Finally, to help mitigate the potential impact of this incident on you, we are 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 12 months from the date of enrollment when changes occur to your credit file. These alerts are sent to you the same day that the change or update takes place with the bureau. These services include proactive fraud assistance and help with any questions that you might have related to protecting your identity. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

P 0000101102G0500

What You Can Do. 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: [redacted]. The deadline to enroll in these services is 90 days from the date of this letter.

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.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions about this letter or need assistance, please call our dedicated team with Cyberscout at [redacted] Cyberscout representatives are available Monday through Friday from 8:00 am - 8:00 pm Eastern Time. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

Calton & Associates, Inc.

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 incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

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 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 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.

Residents of the below states can obtain additional information or take additional steps to avoid identity theft:

- ***District of Columbia residents:*** District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; oag@dc.gov; 202-727-3400.
- ***Maryland residents:*** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https:// www.marylandattorneygeneral.gov/or 1-410-528-8662 or 1-888-743-0023.
- ***Massachusetts residents:*** Under Massachusetts law, you have the right to file a police report.
- ***New York residents:*** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.
- ***North Carolina residents:*** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***Rhode Island residents:*** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag. ri.gov or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately [XX] Rhode Island residents potentially impacted by this incident.

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Calton & Associates
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

June 26, 2025

Subject: Notice of Data Security Incident

Dear [redacted]

At Calton & Associates, your trust is our highest priority, and we are deeply committed to safeguarding the privacy and security of your personal information. We are writing to inform you of a recent data security incident that involved your personal information, and to assure you that we have taken swift, decisive action to address it. This letter provides details about the incident, the robust steps we are taking to protect you, and resources available to help protect your personal information, giving you peace of mind.

What Happened. On April 25, 2025, we determined some of your information was involved in the subject incident. The incident and our response efforts began on March 28, 2025, when we experienced a network disruption and started investigating immediately, with support from cybersecurity. From the investigation, we determined unauthorized individuals accessed our network on March 28, 2025 and took certain files during this window. We conducted a meticulous review of those files to determine what information was accessible to the unauthorized individuals and discovered some of your personal information was contained within the potentially affected data which is the reason for this notification. Please rest assured that throughout our investigation, review, and mitigation, your best interest was our top priority.

What Information Was Involved. The information may have included your Name, address, social security number, and account number. Please note that we have no evidence of any misuse, or attempted misuse, of any information due to the incident. The security of your information remains our top concern, and we are taking every precaution to ensure it stays that way.

What We Are Doing. Upon identifying the incident, we took immediate steps to ensure the unauthorized individuals no longer had access to our network. Furthermore, to enhance network security and to minimize the risk of a similar incident occurring in the future, we implemented additional cybersecurity measures. We reported the event to the FBI and are fully cooperating with their investigation. Finally, to help mitigate the potential impact of this incident on you, we are 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 12 months from the date of enrollment when changes occur to your credit file. These alerts are sent to you the same day that the change or update takes place with the bureau. These services include proactive fraud assistance and help with any questions that you might have related to protecting your identity. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

P 0000101102G0500

What You Can Do. 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: [redacted]. The deadline to enroll in these services is 90 days from the date of this letter.

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.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions about this letter or need assistance, please call our dedicated team with Cyberscout at [redacted] Cyberscout representatives are available Monday through Friday from 8:00 am - 8:00 pm Eastern Time. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

Calton & Associates, Inc.

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 incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

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 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 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.

Residents of the below states can obtain additional information or take additional steps to avoid identity theft:

- ***District of Columbia residents:*** District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; oag@dc.gov; 202-727-3400.
- ***Maryland residents:*** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https:// www.marylandattorneygeneral.gov/or 1-410-528-8662 or 1-888-743-0023.
- ***Massachusetts residents:*** Under Massachusetts law, you have the right to file a police report.
- ***New York residents:*** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.
- ***North Carolina residents:*** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***Rhode Island residents:*** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag. ri.gov or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately [XX] Rhode Island residents potentially impacted by this incident.

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.