



Lauren Godfrey, Partner
Cybersecurity & Data Privacy Team
322 North Shore Drive, Building 1B
Suite 200
Pittsburgh, PA 15212
lgodfrey@constangy.com
Mobile: 973.462.9521

February 29, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notification of Data Security Incident

Dear Attorney General Frey:

This letter is to provide an update regarding the recent data security incident experienced by Brady Martz & Associates ("Brady Martz") described in our previous correspondence dated September 8, 2023.

On February 29, 2024, Brady Martz mailed notification letters to one additional Maine resident whose information may have been involved in this incident. The information varies depending on the individual, but may include individuals' names, dates of birth, addresses, telephone numbers, health insurance information, medical information, and Social Security numbers. The letter includes information notifying them of the incident, offering complimentary identity protection services to those whose Social Security numbers were affected, and providing additional steps they can take to protect their information. A copy of the sample notification letter is enclosed.

If you have any questions or need additional information, please do not hesitate to contact me at by phone 412.870.4129 or by email at lgodfrey@constangy.com.

Regards,

A handwritten signature in blue ink that reads "Lauren Godfrey". The signature is written in a cursive style.

Lauren Godfrey
Partner

Enc.: Sample Consumer Notification Letter



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Via First-Class Mail

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

To Enroll, Please Visit: www.equifax.com/activate Enrollment Code: <<Activation Code>>
--

<<Date>>

Notice of Data <<Variable Data 1>>

Dear <<Name 1>> ,

We are writing to inform you of a cyber incident experienced by Brady Martz & Associates PC (“Brady Martz”) that may have impacted your personal information. As part of our response to the cyber incident, we are notifying you of the incident and providing you with information and resources you can use to further protect your information, including free credit monitoring being offered by Brady Martz.

What Happened: On November 19, 2022, we, Brady Martz, became aware of unusual activity occurring within our digital systems. We immediately took steps to secure our digital systems and engaged independent cybersecurity experts to help us investigate the incident and assess the extent, if any, of unauthorized access. As a result of this investigation, we concluded that an unauthorized third party may have acquired information from a limited portion of our systems, including information we have received from or on behalf of some of our clients.

After a thorough review of the information involved in this incident, we were able to verify the nature and extent of personal information involved in the incident. As a result, we have determined that your personal information may have been affected. Additionally, we have determined that your information was likely in our possession due to certain financial services Brady Martz provides to Family HealthCare Center located in Fargo, North Dakota (and surrounding locations).

What Information Was Involved: It is possible that the following information may have been accessed or acquired by an unauthorized third party during the incident: your name, date of birth, address, telephone number, Social Security Number, health insurance information, and certain medical information such as patient account number, diagnosis and treatment information, physician name, date(s) of service, and costs associated with treatment. However, we have no evidence that your information, or the information of others, has been misused as a result of the incident.

As indicated above, although you may not be familiar with our company, Brady Martz is an accounting, auditing, and related services company. To perform services for our clients, we generally work with information related to our clients’ employees and/or patients. In this case, the results of our investigation indicate that we likely acquired your information while performing certain services for our client, Family HealthCare Center.

What We Are Doing: The security of the information in our possession is a top priority for Brady Martz. Upon discovering the incident, we promptly took steps to mitigate any potential impact to our organization and the information we hold, including initiating a forensic investigation with the assistance of incident response specialists and confirming the security of our internal network and systems. Additionally, we have implemented enhanced technical security measures and monitoring designed to prevent similar incidents from occurring in the future. We

also notified the FBI and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

As a further precaution, we are offering you <<CM Duration>> months of complimentary identity monitoring services through Equifax. This service helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. In addition, you can also enroll in Equifax's complimentary credit and identity monitoring services by going to the link noted above or calling 844-678-3580. When prompted, please provide the unique code noted above to enroll in the services. The deadline to enroll is <<Enrollment Deadline>>.

As a precautionary measure, we recommend that any individuals impacted by this incident remain vigilant to protect against fraud and/or identity theft by, among other things, reviewing your financial account statements and monitoring free credit reports. If you detect any suspicious activity on an account, promptly notify the institution or company with which the account is maintained or law enforcement authorities in the case of suspected identity theft. Additionally, we are offering you complimentary credit monitoring services for any individuals potentially impacted by this incident. If you wish to receive these services, instructions on how to enroll in these services are included in this letter, along with additional information regarding the resources available to you, and the steps that you can take to further protect your information.

For More Information: If you have any questions or need assistance, please call 844-678-3580 between the hours of 8:00 am and 8:00 pm (CST) Monday through Friday (excluding holidays). You will find additional information regarding the resources available to you and the steps that you can take to further protect your personal information attached to this letter.

The security of the information in our possession is a top priority for Brady Martz and we are committed to maintaining the highest standards of data security. We deeply regret any inconvenience this may cause and want to assure you that we have taken steps to prevent such incidents from happening in the future. Thank you for your understanding and cooperation.

Sincerely,

A handwritten signature in black ink that reads "Brady Martz". The signature is written in a cursive, flowing style.

Brady Martz & Associates PC
24 West Central Avenue
Minot, ND 58702

Steps You Can Take to 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

P.O. Box 105851
Atlanta, GA 30348
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 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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.