



Lauren Godfrey
322 North Shore Drive,
Building 1B, Suite 200
Pittsburgh, PA 15212
lgodfrey@constangy.com
973.462.9521

November 14, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Taylor Odachowski Schmidt & Crossland LLC ("TOSC") in relation to a recent data security incident. TOSC takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. We are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately 1 Maryland resident.

1. Nature of the Security Incident

On March 11, 2024, TOSC was alerted to potential unusual activity within its network. In response, TOSC immediately took measures to secure its network and to commence an investigation to determine the full nature and scope of the event. TOSC engaged cybersecurity experts to assist with the process. TOSC's investigation determined that some data may have been acquired without authorization. We engaged a third party to conduct a comprehensive review of all affected information. After a thorough review of the information, on or about June 26, 2024, we determined that some individuals' personal information was contained in the potentially affected data. TOSC then took steps to locate information needed to effectuate notification to such individuals. At the conclusion of this process on October 9, 2024, TOSC arranged for notification to potentially affected individuals promptly thereafter.

The potentially affected information varies for each individual but may have included individuals' name, Social Security number, US alien registration number, and passport number.

2. Number of Maryland Residents Affected

On November 14, 2024, TOSC notified approximately 1 Maryland resident within the potentially affected population, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

11982184v1

12014589v1

3. Steps Taken Relating to the Incident

As soon as TOSC learned of the unusual network activity, it took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. TOSC has implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

TOSC is providing those whose Social Security number was involved with identity protection services through TransUnion. The TransUnion identity protection services include Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services and fraud assistance at no charge for 12 months. In addition, TOSC has established a toll-free call center through TransUnion to answer questions about the incident and address related concerns.

Additionally, TOSC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TOSC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

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

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter

Taylor Odachowski Schmidt & Crossland LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



November 11, 2024

Subject: Notice of Data security incident

Dear [REDACTED],

I am writing to inform you of a recent incident that may have affected some of your personal information. Taylor Odachowski Schmidt & Crossland LLC ("TOSC") is committed to maintaining the privacy and security of all information in our possession. This letter includes information about the incident and provides you with steps you can take to protect your personal information, along with a complimentary offer of credit and identity monitoring services.

What happened? On March 11, 2024, TOSC was alerted to potential unusual activity within our network. In response, we immediately took measures to secure our network and to commence an investigation to determine the full nature and scope of the event. TOSC engaged cybersecurity experts to assist with the process. Our investigation determined that some data may have been acquired without authorization. We engaged a third party to conduct a comprehensive review of all affected information. After a thorough review of the information, on or about June 26, 2024, we determined that some of your personal information was contained in the potentially affected data. TOSC then took steps to locate information needed to effectuate notification to such individuals. At the conclusion of this process on October 9, 2024, TOSC arranged for notification to potentially affected individuals.

What Information Was Involved? The potentially affected information included your name and Social Security number.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We also performed a thorough review of our systems to investigate the incident and ensure that our systems remain secure. TOSC implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. TOSC also notified the Federal Bureau of Investigation of the incident and will provide whatever cooperation is necessary to hold the perpetrators accountable.

In addition, we have secured the services of TransUnion to provide credit monitoring and identity theft restoration services at no cost to you. These services include 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 twelve 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 the 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.

To enroll in these 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]

000010102G0400

P

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.

What You Can Do: Receiving this letter does not mean that you are the victim of identity theft. We recommend that you activate your complimentary services using the membership number provided above. We also recommend that you review the guidance included with this letter about how to protect your information.

For More Information: If you have any questions about this letter, please contact our dedicated call center for this incident at **1-800-405-6108**. Representatives are available Monday through Friday from 8:00 am - 8:00 pm Eastern Time, excluding holidays, and have been fully versed on this incident.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in dark ink, appearing to read "Peter H. Schmidt, II". The signature is fluid and cursive, with the last name "Schmidt" being more prominent.

Peter H, Schmidt, II
Taylor Odachowski Schmidt & Crossland LLC
300 Oak St., Ste 200,
Saint Simons Island, GA 31522

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 (the “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 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 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 877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 www.marylandattorneygeneral.gov/Pages/CPD 888-743-0023	Oregon Attorney General 1162 Court St., NE Salem, OR 97301 www.doj.state.or.us/consumer-protection 877-877-9392
California Attorney General 1300 I Street Sacramento, CA 95814 www.oag.ca.gov/privacy 800-952-5225	New York Attorney General The Capitol Albany, NY 12224 800-771-7755 ag.ny.gov	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400



Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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.