

March 23, 2023

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents Norberg, Davis, Bourne & Painter, LLP ("NDBPLLP") located in Silver Spring, Massachusetts, with respect to a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

1. Nature of the Security Incident

In March 2023, NDBPLLP discovered fraudulent tax forms filed on behalf of certain individuals. In response, NDBPLLP immediately retained independent cybersecurity experts to conduct a forensic investigation to determine whether any personal information may have been accessed or acquired.

Based on that investigation, on March 29, 2023, NDBPLLP learned that an unauthorized actor accessed a single file containing personal information. NDBPLLP then worked diligently to identify individuals whose information may have been impacted, as well as current address information to effectuate notification.

NDBPLLP is notifying all potentially impacted individuals of the incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

2. Number of Maryland Residents Affected & Information Involved

On May 23, 2023, NDBPLLP notified thirteen (13) Maryland residents of this incident via first class U.S. mail. The information involved in the incident includes Maryland residents' names, driver's license numbers, and Social Security numbers. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

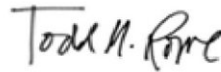
In response to the incident, NDBPLLP retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. NDBPLLP also implemented additional security measures to further harden its email environment in an effort to prevent a

similar event from occurring in the future. Additionally, NDBPLLP has reported the incident to the FBI and will cooperate with any resulting investigation. Finally, NDBPLLP is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

4. Contact Information

NDBPLLP takes seriously its responsibility to protect the security of the information it maintains. If you have any questions or need additional information, please do not hesitate to contact me at 312.520.2521 or by email at trowe@constangy.com.

Regards,

A handwritten signature in black ink that reads "Todd N. Rowe". The signature is written in a cursive, slightly slanted style.

Todd Rowe
Partner

Enc.: Sample Consumer Notification Letter

NORBERG, DAVIS, BOURNE & PAINTER, LLP

CERTIFIED PUBLIC ACCOUNTANTS

12069 Tech Road
Silver Spring, MD 20904

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<Variable1>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

<<Date>>

Subject: Notice of Data Security Incident

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

Norberg, Davis, Bourne & Painter, LLP (“NDBPLLP”) is writing to inform you of a data security incident that may have involved your personal information. NDBPLLP takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information, including an offer for you to enroll in credit monitoring and identity protection services at no cost to you.

What Happened? On March 7, 2023, NDBPLLP discovered fraudulent tax forms filed on behalf of certain individuals. With the assistance of independent cybersecurity experts, we immediately initiated an investigation. Based on that investigation, on March 29, 2023, we learned that an unknown actor accessed a file which contained personal information. We then took steps to identify current mailing addresses for such individuals in order to effectuate notification.

What Information Was Involved? The information that may have been impacted includes your name and <<Variable2>>.

What Are We Doing? As soon as we discovered this incident, we took the steps referenced above and implemented additional security features to reduce the risk of a similar event occurring in the future. We notified the Federal Bureau of Investigation (“FBI”) and have been in contact with the Internal Revenue Service (“IRS”) to provide relevant information about this incident and will continue to provide whatever cooperation is necessary to hold the perpetrator(s) of this incident accountable.

Additionally, NDBPLLP is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: twenty-four (24) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

The deadline to enroll in these services is August 30, 2023. With this protection, IDX will help to resolve issues if your identity is compromised.

What Can You Do? You can follow the recommendations on the following page to help protect your personal information. NDBPLLP also encourages you to enroll in the services being offered at no cost to you through IDX by using the enrollment code provided above.

For More Information: If you have additional questions, please call Philip Bourne at 301-680-8900. Further information about how to protect your personal information appears on the following page. If you need assistance with enrollment, please call IDX at 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect>. You will need to reference the enrollment code listed above.

Protecting your information is important to us. Please know that NDBPLLP takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeremy Stark", with a stylized, cursive script.

Jeremy Stark, Partner
Norberg, Davis, Bourne & Painter, LLP

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 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. 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 as follows:

- *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.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>