

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
kevin.scott@gtlaw.com

June 11, 2024

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Dear Attorney General Brown:

We represent Santoro & Whitmire (“S&W”) located at 10300 W Charleston Blvd, Suite 13-246, Las Vegas, NV 89135, and are writing to notify your office of an incident that may affect the security of some personal information relating to 29 Maryland residents.

Recently, after the firm permanently closed its business, S&W was the target of a ransomware attack. S&W immediately notified law enforcement, moved quickly to contain the incident, and conducted a thorough investigation with the assistance of computer forensic experts. While S&W believes it is likely the attacker only wanted money and not the information on its computers, in an abundance of caution, they are notifying the entire data population that their information may have been accessed by the attackers.

On May 03, 2024, S&W discovered that data containing personal information was exfiltrated from its IT environment. While S&W has no reports of misuse of anyone’s information, its investigation revealed that the system may have contained information relating to personal information, and it took time to identify those persons affected. The information may have included individuals’ name and Social Security number.

The security of all information in S&W’s systems is taken very seriously, and they want to assure that there are already steps in place to prevent a reoccurrence, including enhanced security measures and enhanced oversight of third-party vendors. Additionally, S&W is offering individuals one year of identity protection (credit monitoring and identity theft) services from IDX/ZeroFox.

On or about June 11, 2024, S&W began mailing notifications to all potentially affected individuals. An example of the notification is attached. Notification has also been made to the three major credit reporting agencies.

Attorney General Brown

June 11, 2024

Page 2

Should you have any questions regarding this notification or other aspects of the data security event, please contact me for any additional information.

Best Regards

A handwritten signature in blue ink, appearing to read "Kevin M. Scott", with a long horizontal flourish extending to the right.

Kevin M. Scott
Shareholder

Santoro Whitmire

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

June 11, 2024

<<Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident that may have impacted some of your personal information. We take the security of your information and any concern this incident may cause very seriously. This letter contains information about actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened

Recently, after the firm permanently closed its business, we were the target of a ransomware attack. Ransomware is a computer virus that encrypts computer systems until and unless we pay money (i.e., the ransom) demanded by the attackers. We immediately notified law enforcement, moved quickly to contain the incident, and conducted a thorough investigation with the assistance of computer forensic experts. We believe it is likely the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that your information may have been accessed by the attackers.

What Information Was Involved

On May 8, 2024, our investigation revealed that some documents accessed may have contained information relating to personal information, and it took time to identify those persons affected. The information may have included your<<Variable Text 1>>. We are notifying you in an abundance of caution.

What We Are Doing

The security of all information in our systems is taken very seriously, and we want to assure you that there are already steps in place to prevent a reoccurrence, including enhanced security measures and enhanced oversight of third-party vendors. Although we have no indications of fraudulent activity, out of an abundance of caution, we have secured the services of IDX, a ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<1 year/2 year>> 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.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 259-8122 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is September 11, 2024.

Although we have no reports of misuse of your or anyone's information, we encourage you to follow the instructions in this letter and enroll in the identity protection services we are providing at no cost to you. We also recommend that you review the "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (888) 259-8122 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. Protecting your information is important to us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

James Whitmire

Important Additional Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were 5 Rhode Island residents notified in this incident.

DC Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Attorney General
400 6 th Street NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain or file a police report.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

www.equifax.com/personal/credit-report-services/credit-freeze/

1-866-478-0027

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013-9544

<http://www.experian.com/freeze/center.html>

1-888-397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

www.transunion.com/credit-freeze