



Maria Efaplatidis
77 Water Street, Suite 2100
New York, NY 10005
Maria.Efaplatidis@lewisbrisbois.com
Direct: 212.232.1366

January 3, 2022

VIA Electronic Mail

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
Email: Idtheft@oag.state.md.us

Re: Data Security Incident Notice

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Schochor Federico & Staton, P.A. (Schochor) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

1. Nature of the Security Incident

Schochor is a law firm based in Baltimore, Maryland.

On June 23, 2021, Schochor discovered unusual activity within its Microsoft Office 365 environment. Immediately upon discovery, Schochor took steps to secure its email environment. Additionally, Schochor retained cybersecurity and digital forensics experts as well as incident response counsel to assist with its response efforts and conduct an investigation to determine the source and scope of the incident.

The investigation revealed that an unauthorized actor was able to access one Schochor e-mail account. Further, on November 23, 2021, the investigation determined personal information may have been impacted as a result of the incident. Schochor then worked diligently to identify the individuals impacted and the address information associated with such individuals in order to provide notification of this incident. This process was completed on December 9, 2021.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for 153 Maryland residents. The information involved Social Security Numbers, Driver License, Health Information, Health Insurance, and Medical Information.

The affected individual will receive a letter notifying them of the incident and providing additional steps they can take to protect their personal information. For individuals whose Social Security numbers were potentially impacted, Schochor will be offering complimentary identity monitoring services. The notification letters will be sent via USPS First Class Mail on January 4, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. Measures Taken to Address the Incident

In response to the incident, Schochor retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise.

Additionally, as discussed above, Schochor is notifying the affected individual and providing them with steps they can take to protect their personal information.

4. Contact Information

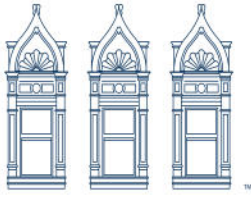
Schochor is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Maria Efaplatidis at Maria.Efaplatidis@lewisbrisbois.com.

Sincerely,



Maria Efaplatidis of
LEWIS BRISBOIS BISGAARD & SMITH LLP

cc: Schochor Federico and Staton, P.A.



SCHOCHOR, FEDERICO
AND STATON, P.A.

May 6, 2022

«First_Name_or_Initial» «Middle_Name_or_Initial» «Last_Name»

«Address_1», «Address_2»

«City», «State» «Zip_Code»

Re: Notice of Data Security Incident

To Enroll, Please Call:

1-800-939-4170

Or Visit:

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

Enrollment Code: CODE

Dear «First_Name_or_Initial» «Last_Name»,

We are writing to inform you of a data security incident experienced by Schochor Federico & Staton, P.A. ("SFSPA"), that may have affected your personal information. Your information was provided to us by a client of our firm in relation to providing our legal services. As explained below, we recently learned that an unauthorized individual gained access to a SFSPA employee email account and may have accessed your information contained in the account. We are writing to notify you of this incident, to offer you complimentary identity monitoring and protection services, and to inform you about steps that can be taken to help protect your personal information.

What Happened? On June 23, 2021, we detected unusual activity relating to a SFSPA employee's email account. Upon discovering this activity, we took steps to secure our email system and launched an investigation to determine the extent of the incident. We also engaged a digital forensics firm to assist in our investigation and help assess whether any sensitive information may have been accessed or acquired without authorization. Through this investigation, we determined that unauthorized access to the employee's email account occurred. Following this, we then conducted a comprehensive review of the contents of the impacted email account to determine what, if any, sensitive data might have been affected. On November 23, 2021, we discovered that the incident may have impacted your information and the information of a limited number of other individuals. We then worked diligently to identify up-to-date address information to notify you and the other impacted persons.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems.

What Information Was Involved? The information involved may have included your name, all data tag.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above and took steps to secure the impacted email account. We also implemented measures to help prevent a similar incident from occurring in the future. Finally, out of an abundance of caution, we are now offering you complimentary identity protection services through IDX, a data security and recovery services expert. Your complimentary one-year enrollment in IDX identity protection includes: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter.

What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your personal information. You can also enroll in the IDX identity protection services being provided to you, at no cost, through IDX. To enroll, please call **1-800-939-4170** or visit the IDX website at **<https://app.idx.us/account-creation/protect>** and provide your enrollment code located at the top of this page. Please note that the deadline to enroll is **March 31, 2022**. Additional information describing the IDX identity protection services, along with other recommendations to protect your personal information, is included with this letter.

For More Information: If you have questions or need assistance, please call Phone Number, Monday through Friday from 9 a.m. to 5 p.m. ET. Please have your Enrollment Code ready.

Protecting your information is important to us. Please know that we take this incident very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Kerry', with a stylized flourish at the end.

Kerry D. Staton, Founding Partner
Schochor, Federico and Staton, P.A.

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 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 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:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.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 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. 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: Under U.S. law, 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. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 www.ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400

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 others. 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



One-Year Enrollment in IDX Identity Protection

Website and Enrollment. Please visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at **1-800-939-4170** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.