octillo
LEGAL + TECH

Liberty Building, 420 Main Street, Suite 1110, Buffalo, New York 14202
75 S. Clinton Ave, 510 Clinton Square, Suite 555, Rochester, New York 14604
3 Columbus Circle, #1500, New York, New York 10019
600 Broadway, Suite 700, San Diego, California 92101
2 Bala Plaza, Suite 300, #704, Bala Cynwyd, Pennsylvania 19004

July 29, 2022

VIA CERTIFIED MAIL
Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

On behalf of Smolin Lupin, ("Smolin"), this letter provides notice of a recent data security incident pursuant to N.H. Rev. Stat. Ann. §359-C:20. By providing this notice, Smolin does not waive any rights or defenses regarding the applicability of New Hampshire law, and the applicability of the New Hampshire data notification laws or personal jurisdiction.

On March 30, 2022, Smolin became aware of suspicious activity in an employee's email account (the "Incident"). Upon discovering the suspicious activity, Smolin immediately began an investigation and took steps to contain and remediate the situation, including changing passwords, adopting new security measures in addition to its existing safeguards, and engaging data security experts to assist. The investigation found that an unauthorized actor gained access to an employee's email account and then leveraged that email account to access a program used to store data for preparing tax returns. Upon further investigation, Smolin determined that the unauthorized actor copied or downloaded documents from that program relating to 2020 income tax returns and 2021 tax data.

After discovering the suspicious activity, Smolin immediately notified law enforcement and tax authorities. Smolin has since worked closely with the Internal Revenue Service to share information and take steps to protect our clients' Information. Likewise, Smolin has shared information with the state tax divisions in each relevant state. On April 25, 2022, Smolin provided initial notice of the Incident and offered two years of no-cost credit monitoring from Experian IdentityWorks to potentially affected individuals.

At the same time, Smolin continued to work closely to tax authorities and complete its investigation. The investigation determined that the information potentially accessed by the unauthorized actor included first and last names, social security numbers, driver's license numbers and other state identification numbers, passport numbers, dates of birth, financial account, and payment card information. Note that this list describes general categories of information involved in this Incident and that not all data elements were present for each potentially affected individual.

Three (3) New Hampshire residents may have been affected the Incident. On August 2, 2022, Smolin will provide additional written notice to potentially affected individuals, including the New Hampshire residents. A copy of this letter is attached for reference.

Please feel free to contact me with any questions at 716-898-2102 or dgreene@octillolaw.com.

Sincerely,

Daniel P. Greene, Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encl.

[redacted]

[redacted]

Dear [redacted]:

In April 2022, we wrote to advise you that Smolin Lupin ("Smolin") recently experienced a data security incident (the "Incident") that may have affected your personal information ("Information") and provided a code for you to sign up for two (2) years of cost-free credit monitoring services through Experian IdentityWorks. We are writing now to provide an update on our investigation and remediation of the Incident, and, as a precaution, provide you with further resources and steps you can take to protect your Information.

What Happened?

On March 30, 2022, we discovered suspicious activity in an employee's email account. Upon discovering the suspicious activity, we immediately began an investigation. We took steps to contain and remediate the situation, including changing passwords, adopting new security measures in addition to our robust protections, and engaging data security experts to assist. The investigation found that an unauthorized actor gained access to an employee's email account, and then leveraged that email account to access a program used to store data for preparing tax returns. Upon further investigation, we determined that the unauthorized actor copied or downloaded documents from that program relating to 2020 income tax returns and 2021 tax data. Our investigation found that your Information may have been included in the information that the unauthorized actor downloaded.

What Information Was Involved?

Our investigation revealed the information that the unauthorized actor potentially accessed included first and last names, social security numbers, driver's license numbers and other state identification numbers, passport numbers, dates of birth, and/or financial account and payment card information. Note at this describes general categories of Information involved in this Incident and may include categories that are irrelevant to you.

What We Are Doing.

After discovering the suspicious activity, we immediately notified law enforcement and tax authorities. We have since worked closely with the Internal Revenue Service to share information and take steps to protect our clients' Information. Likewise, we have shared information with the state tax divisions in each relevant state. We provided the option to sign up for two (2) years of no-cost credit monitoring from Experian IdentityWorks to interested potentially affected individuals and will continue to

communicate with tax authorities on our clients' behalf closely. Internally, we have added additional security measures to our existing protections and have worked to strengthen our systems and practices further to prevent similar events from occurring in the future.

What You Can Do.

As a reminder, experts encourage simple steps for protecting your personal information, including changing your passwords regularly, monitoring your personal accounts closely, reporting suspicious activity, and never sharing your personal information with unknown or untrusted sources. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

For More Information.

If you have additional questions related to this matter, please call your Smolin engagement partner or the undersigned.

Sincerely,

Henry Rinder

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Complimentary Experian IdentityWorks Credit Monitoring. Once you enroll in Experian IdentityWorks, you can contact Experian immediately regarding any fraud issues, and have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. [2]

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.oag.state.md.us, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800- 964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, https://ag.ks.gov/, 1-800-432-2310.

For Kentucky residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1- 401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800- 621-0508.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

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

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.