

March 1, 2023

Attorney General John M. Formella
New Hampshire Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Formella:

Pursuant to N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21, we are writing to notify you of an incident involving unauthorized access of personal information for 1 New Hampshire resident.

Nature of the Unauthorized Access

On or about January 18, 2023, Radkl US LLC and its affiliates ("Radkl") became aware there had been unauthorized access to one user account in Microsoft Office 365, including portions of Radkl's Microsoft Sharepoint site (a web-based collaborative platform), and two people within Radkl were targeted with a spoofed email for a fraudulent corporate wire transfer request. It is estimated that the unauthorized access first occurred on or about January 10, 2023 and continued through January 18, 2023. This incident involved unencrypted personal information in electronic form, including name, social security number, date of birth, employee ID, tax status, salary information, start date, title, work location, and other related information maintained for HR purposes.

New Hampshire Residents Affected

The 1 affected resident will receive notification shortly pursuant to N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21 via written notice. Please find enclosed a copy of the notice to 1 affected resident.

Steps Radkl Is Taking Relating to the Incident

Radkl took action to successfully secure its systems immediately upon becoming aware of the unauthorized access and spoofing attempt, and is continuing to review its cybersecurity and cyber incident response policies and procedures. Radkl is hereby alerting the New Hampshire Office of the Attorney General. Radkl is providing notification to all affected individuals within one (1) day from the date of this letter, and is offering free identity theft prevention and mitigation services for 12 months to all affected individuals.

Contact Information

Should you have any questions, please contact Nicole Jurayon, Chief Compliance Officer, at

Sincerely,

Kay Smith
Associate General Counsel



Radkl US LLC and Affiliates
40 Wall Street, Floor 38
New York, NY 10005
212-317-7130

Date: March 1, 2023

[name]
[address]
[city, state, zip]

NOTICE OF DATA BREACH

Dear [name]:

We are writing to tell you about a situation involving unauthorized access to some of your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances, steps we are taking in response, and resources we are making available to you.

What Happened?	On or about January 18, 2023, Radkl US LLC and its affiliates ("Radkl") became aware there had been unauthorized access to one user account in Microsoft Office 365, including portions of Radkl's Microsoft Sharepoint site (a web-based collaborative platform), and two people within Radkl were targeted with a spoofed email for a fraudulent corporate wire transfer request. It is estimated that the unauthorized access first occurred on or about January 10, 2023 and continued through January 18, 2023.
What Information Was Involved?	This incident involved your unencrypted personal information in electronic form, including your name, social security number, date of birth, employee ID, tax status, salary information, start date, title, work location, and other related information maintained for HR purposes.
What We Are Doing.	Radkl took action to successfully secure its systems immediately upon becoming aware of the unauthorized access and spoofing attempt, and is continuing to review its cybersecurity and cyber incident response policies and procedures. We are offering free identity theft prevention and mitigation services for 12 months. We have appended to this letter instructions for signing up for this service.
What You Can Do.	<p>The Federal Trade Commission ("FTC") recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus (please find contact information listed below). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.</p> <p>Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. When you receive a credit report from each agency, review the reports</p>

	<p>carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. These can be signs of identity theft. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.</p> <p>Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:</p> <p>Annual Credit Report Request Service P.O. Box 1025281 Atlanta, GA 30348-5283</p> <p>We strongly advise that you consider placing a free credit freeze with all three major credit bureaus. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers below. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.</p> <p>You may also want to consider a dark web scan. A one-time dark web scan is offered for free by Experian at https://www.experian.com/consumer-products/free-dark-web-email-scan.html.</p> <p>We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.</p>
<p>Other Important Information.</p> <p>Please note the toll-free telephone numbers and addresses of the three major credit reporting agencies:</p> <p>Equifax P.O. Box 740241 Atlanta, GA 30374 equifax.com/personal/credit-report-services or 1-800-685-1111</p> <p>Experian P.O. Box 9532</p>	

Allen, TX 75013
experian.com/help or 1-888-397-3742

TransUnion

P.O. Box 2000
Chester, PA 19016
transunion.com/credit-help or 1-800-888-4213

You can obtain more information from the following sources about steps you can take to avoid identity theft:

Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580

The FTC provides information online at consumer.ftc.gov/features/identity-theft and has an identity theft hotline at 877-438-4338 (TTY: 1-866-653-4261).

For residents of California: You may obtain information about preventing and avoiding identity theft from the California Office of the Attorney General, P.O. Box 944255, Sacramento, CA 94244-2550, 1-800-952-5225, <https://oag.ca.gov/>.

For residents of New Hampshire: You may obtain information about preventing and avoiding identity theft from the New Hampshire Office of the Attorney General, 33 Capitol Street, Concord, NH 03301, 1-888-468-4454, <https://www.doj.nh.gov/>.

For residents of New York: You may obtain information about preventing and avoiding identity theft from the New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

For More Information.	We sincerely regret any inconvenience this incident might cause you. If you have any questions, please contact us by phone at 212-317-7130 or by e-mail at rsheftel@radkl.io .
------------------------------	---

Sincerely,

Ryan Sheftel
CEO



What information was lost or exposed?


▼ Social Security number

- ☐ If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
 - ☐ Get your free credit reports from annualcreditreport.com . Check for any accounts or charges you don't recognize.
 - ☐ Consider placing a [credit freeze](#) . A credit freeze makes it harder for someone to open a new account in your name.
 - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.
 - If you decide not to place a credit freeze, at least consider [placing a fraud alert](#) .
 - ☐ Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
 - ☐ Don't believe anyone who **calls** and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
 - ☐ Continue to check your credit reports at annualcreditreport.com . You can order a free report from each of the three credit reporting companies once a year.
-


▼ Online login or password

- ☐ Log in to that account and change your password. If possible, also change your username.
 - If you can't log in, contact the company. Ask them how you can recover or shut down the account.
- ☐ If you use the same password anywhere else, change that, too.
- ☐ Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.



▼ Debit or credit card number

- ☐ Contact your bank or credit card company to cancel your card and request a new one.
- ☐ Review your transactions regularly. Make sure no one misused your card.
 - If you find fraudulent charges, call the fraud department and get them removed.
- ☐ If you have automatic payments set up, update them with your new card number.
- ☐ Check your credit report at annualcreditreport.com .

▼ Bank account information

- ☐ Contact your bank to close the account and open a new one.
- ☐ Review your transactions regularly to make sure no one misused your account.
 - If you find fraudulent charges or withdrawals, call the fraud department and get them removed.
- ☐ If you have automatic payments set up, update them with your new bank account information.
- ☐ Check your credit report at annualcreditreport.com .

▼ Driver's license information




- ☐ Contact your [nearest motor vehicles branch](#)  to report a lost or stolen driver's license. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a duplicate.
- ☐ Check your credit report at annualcreditreport.com .

▼ Children's personal information

- ☐ Request a credit freeze for your child — [if this service is available in your state](#). A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions for each credit bureau:

- [Equifax](#) 
- [Experian](#) 
- [Transunion](#) 

- ☐ No matter what state you live in, you can check to see if your child has a credit report. Each bureau has specific instructions for these requests:

- [Equifax](#) 
- [Experian](#)  (Click on "Minor Child Instructions" under "Information You Should Know")
- [Transunion](#) 

- ☐ If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove fraudulent accounts.

- ☐ Review the FTC's information on [Child Identity Theft](#) .

Dear [name]:

Radkl US LLC and its affiliates ("Radkl") have retained **NortonLifeLock** to provide 1 year of complimentary **LifeLock Defender™ Preferred** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **Norton.com/offers**.
2. Below the THREE protection plan boxes, you may enter the **Promo Code:** [promo code] and click the "APPLY" button.
3. Your complimentary offer is presented. Click the Orange "START MEMBERSHIP" button.
4. A Popup will appear to enter your Member ID [member ID] and click "APPLY"
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: 800-899-0180

You will have until April 30, 2023 to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Defender™ Preferred** membership includes:

- ✓ Primary Identity Alert System[†]
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring^{**}
- ✓ Norton™ Security Deluxe² (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to \$25,000^{†††}
- ✓ Personal Expense Compensation up to \$25,000^{†††}
- ✓ Coverage for Lawyers and Experts up to \$1 million^{†††}
- ✓ U.S-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores^{1**}
The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring^{1**}
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts^{†††}

¹If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment. No one can prevent all identity theft or cybercrime. [†] LifeLock does not monitor all transactions at all businesses.

² Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

^{**}These features are not enabled upon enrollment. Member must take action to get their protection.

^{†††} Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Defender Preferred. And up to \$1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.