C A D W A L A D E R

March 30, 2023

U.S. MAIL

Office of the Attorney General
Consumer Protection Bureau
33 Capitol St.
Concord, NH 03301

RECEIVED

APR 0 4 2023

CONSUMER PROTECTION

Dear Sir or Madam:

On behalf of Cadwalader, Wickersham & Taft ("Cadwalader"), this letter provides notice of a cybersecurity incident involving six New Hampshire residents. By way of background, Cadwalader is an international law firm based in New York.

We first detected a cybersecurity incident disrupting portions of our network on November 16, 2022. Upon discovery, we immediately took all systems offline as a precaution to contain the incident. That same day, we launched an investigation with the assistance of outside experts, began notifying our clients, and notified law enforcement.

Upon identifying the affected data set, Cadwalader began working to identify all personal information involved in order to carry out notifications pursuant to applicable law. On February 28, 2023, Cadwalader determined that the personal information associated with six New Hampshire residents was affected by this incident. The types of personal information potentially affected include ,

Cadwalader began sending these individuals notice on March 30, 2023, via U.S. mail. A draft of the notification letter is enclosed. As stated in the attached draft notice, Cadwalader has engaged Kroll Information Assurance, LLC to provide two years of identity monitoring services at no cost to the individuals. The identity monitoring services include fraud consultation and identity theft restoration services. We have also established a call center to respond to questions.

Cadwalader takes the protection of personal information seriously, and is committed to answering any questions that you may have. Please do not hesitate to contact me at

Respectfully yours,

Beth Taylor
General Counsel

CADWALADER

Cadwalader, Wickersham & Taft LLP
200 Liberty Street, New York, NY 10281
Tel +1 212 504 6000 Fax +1 212 504 6666
www.cadwalader.com

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF SECURITY INCIDENT / NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<middle_name>> <<last_name>>,

We are writing to let you know about a cybersecurity incident involving your personal information held by Cadwalader, Wickersham & Taft LLP. We deeply regret that this has occurred. Keeping personal information safe and secure is very important to us and, as you will see below, we have taken robust steps to address the incident and help protect your interests. Please read this entire letter as it contains information to help keep your information secure.

WHAT HAPPENED?

Between November 15-16, 2022, an unauthorized third party gained remote access to our systems and acquired certain information from our network, including documents containing some of your personal information. <<b2b_text_2 (Employee/Non-employee sentence)>>.

Our investigation has determined that the unauthorized third party acquired some of your personal information, including your <<b2b_text_3 ("name" and data elements)>><<b2b_text_4 (data elements cont.)>><<b2b_text_5 (data elements cont.)>>.

Targeted online monitoring has not revealed any indication that your personal information has been leaked or otherwise misused by the unauthorized third party. If this were to occur, this would expose you to a greater risk of identity theft or fraud, financial loss, and non-material loss.

WHAT WE ARE DOING

Upon learning of this incident, we quickly took steps to stop the unauthorized access and began a thorough forensic investigation with the assistance of outside cybersecurity experts. We have also reported this incident to law enforcement and relevant regulators, as well as taking steps to further strengthen our network.

Although at this time we have no indication of any misuse of your information and our investigation has not identified any suggestion that the unauthorized third-party was targeting your personal information, we have engaged Kroll to provide two years of identity monitoring services at no cost to you. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

WHAT YOU CAN DO

We strongly encourage you to take advantage of the identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your online and financial accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to the proper law enforcement authority.

If you would like to take additional steps to help protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file where relevant.

Once again, we sincerely regret that this incident has occurred and have taken robust steps to address it. If you have any questions about the incident, please contact us at , Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Yours sincerely,

Beth Taylor
General Counsel

Cadwalader, Wickersham, and Taft LLP

Additional Helpful Tips

- You can learn more about how to protect yourself against identity theft by contacting the Federal Trade Commission (FTC) or your state's Attorney General to obtain information including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report. **Federal Trade Commission**, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft
- **Order Your Free Credit Report**: We encourage you to periodically obtain credit reports from the below credit agencies and have fraudulent transactions deleted. To obtain an annual free copy of your credit reports, visit **annualcreditreport.com**, call toll-free at 1-877-322-8228, or contact the major credit reporting agencies. Their contact information is as follows:

Equifax:	**Experian:**	**TransUnion:**
equifax.com	**experian.com**	**transunion.com**
equifax**.com/freeze**	**experian.com/freeze**	**transunion.com/freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-888-909-8872

- **Fraud Alert**: You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert puts creditors on notice that you might be a victim of fraud. Creditors will then follow certain procedures designed to protect you, including contacting you before they open new accounts or change your existing accounts. Placing a fraud alert can protect you but also may delay you when you seek to obtain credit.
- **Security Freeze**: You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.
- **Fraud or Identity Theft**: If you suspect theft, you should file a report to law enforcement, the FTC, or the Attorney General in your state. If you are the victim of fraud or identity theft, you have the right to (1) notify the police and Attorney General of your state; and (2) file a police report relating to the incident and obtain a copy of the report.
- **Federal Fair Credit Reporting Act Rights**: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies (CRAs) use your information. The FTC has summarized consumers' FCRA rights as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to a credit score; you have the right to dispute incomplete or inaccurate information; CRAs must correct or delete inaccurate, incomplete, or unverifiable information; CRAs may not report outdated negative information; access to your file is limited; employers need your consent to receive your reports; you may limit "prescreened" credit and insurance offers based on your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580.
- **State-Specific Notices**. Residents of the following states should review the following information:
  - **For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.
  - **For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.
  - **For New York residents:** You may consider placing a Security Freeze on your credit report. For more information on a Security Freeze or on how to avoid identity theft, contact the New York Department of State Division of Consumer Protection (http://www.dos.ny.gov/consumerprotection/; (800) 697-1220) or the New York State Office of the Attorney General (http://www.ag.ny.gov/home.html; (800) 771-7755).

- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226 to contact other nationwide consumer reporting agencies and to make freeze requests and obtain information on combating identity theft.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.