



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

August 17, 2022

File No. 39395.531

VIA WEB PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notification of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Warner Norcross and Judd, LLP (“WNJ”) in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine’s data breach notification statute.

1. Nature of the Security Incident

WNJ is a provider of legal services located in Michigan.

On October 22, 2021, WNJ learned that unauthorized activity was reported involving some of its systems. Upon discovery, WNJ took immediate steps to secure the environment. In addition, it retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident. Based on the findings from the investigation, WNJ undertook an extensive review of the affected systems to determine what personal information may have been impacted, the individuals to whom the information pertained, and addresses for these individuals.

Although the data review is ongoing, on June 28, 2022, we were able to confirm address information for a subgroup of individuals whose information was impacted and proceeded to provide notice to those individuals out of an abundance of caution.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately 7 Maine residents who were notified via USPS First Class Mail on July 11, 2022. The information involved differ depending on the individual but may include name and Social Security numbers.

On August 5, 2022, a second notification letter was sent to 124 affected individuals notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The notification letter was sent via USPS First Class Mail.

3. Measures Taken to Address the Incident

In response to the incident, WNJ retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. In addition, WNJ is in the process of reviewing its current security protocols and adding additional security measures.

As discussed above, WNJ is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

WNJ 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 Efaploamatidis at Maria.Efaploamatidis@lewisbrisbois.com or 212.232.1366.

Sincerely,



Maria Efaploamatidis of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Consumer Letter



Warner Norcross + Judd LLP

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

To Enroll, Please Call:
(833) 423-2982
Or Visit:
<https://response.idx.us/wnj>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

July 11, 2022

Re: Notice of Data Security Incident

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

Warner Norcross + Judd LLP (“W NJ”) is writing to inform you of a data security incident that may have involved your personal information. You may not have heard of our firm -W NJ- but we provide professional legal services to clients in a wide variety of industries and business sectors and we hold relevant data to serve our clients. We take the privacy and security of your information very seriously. Out of an abundance of caution we are providing identity theft protection to those whose information may have been in our data systems affected by the incident. Below is information about the incident and steps you can take to help protect your personal information, including activating the identity monitoring services we are offering at no cost.

What Happened? On October 22, 2021, W NJ learned that unauthorized activity was reported involving some of our systems. We immediately took steps to secure our network and engaged a digital forensics firm to investigate the cause and scope of the incident. Through data mining and manual review, it was confirmed that your information was among the data that was affected. We then worked diligently to identify up-to-date address information to notify you and the other impacted persons; this process was completed on June 28, 2022. Importantly, W NJ is not aware of any misuse of your personal information due to this incident.

What Information Was Involved? The files that may have been accessed by the unauthorized individual contained your name <<Variable 1>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. In addition, we worked with our experts to try to prevent such an incident from ever happening again. We have also secured the services of IDX to provide credit and identity monitoring at no cost for <<12/24>> months. IDX is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an exposure of personal data. The IDX services include: credit monitoring; identity monitoring; \$1 million in identity theft expense reimbursement insurance; and fraud prevention and resolution support.

To receive credit services, you must enroll and be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing the complimentary IDX services is included with this letter.

Please note you must enroll by October 11, 2022. If you have questions or need assistance, please go to <https://response.idx.us/wnj> or call IDX at (833) 423-2982.

What You Can Do: Please review the enclosed “Steps You Can Take to Protect Your Information” page. It describes additional steps you can take to help safeguard your information, 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. We also encourage you to activate the complimentary identity monitoring services we are making available through IDX.

For More Information: If you have questions or need assistance, please call IDX at (833) 423-2982, Monday through Friday from 9 a.m. to 9 p.m. ET.

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 have caused.

Sincerely,

Nathan W. Steed, Partner
Warner Norcross + Judd, LLP
1500 Warner Building, 150 Ottawa Ave N.W.,
Grand Rapids, MI 49503

Steps You Can Take to Protect Your Information

Website and Enrollment. Go to <https://response.idx.us/wnj> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection 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 (833) 423-2982 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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
1-800-916-8800	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, Oregon, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

**New York
Attorney General**
28 Liberty Street
New York, NY
10005
ifraud@ag.ny.gov
1-212-416-8433

**Maryland Attorney
General**
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

**North Carolina
Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

**Rhode Island
Attorney General**
150 S Main St.
Providence, RI
02903
www.riag.ri.gov
401-274-4400

**Oregon Department
of Justice**
1162 Court Street NE
Salem, OR 97301
1-877-877-9392
www.doj.state.or.us

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