MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 11, 2021

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rakuten USA, Inc. DBA Rakuten Americas ("Rakuten"), located at 800 Concar Drive, San Mateo, CA 94402, and are writing to notify your office of an incident that may affect the security of some personal information relating to nine (9) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Rakuten does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 21, 2021, Rakuten's data security team detected that an employee who was in the process of voluntarily leaving the company had transferred a number of files off their Rakuten-issued computer. As soon as Rakuten learned about this person's actions, Rakuten launched an investigation into the nature and scope of their activity. The investigation revealed that some of these transferred files contained sensitive personal information of employees. This person had been authorized to access this information only on a Rakuten device for assigned work purposes. Rakuten immediately took steps to limit potential further exposure of the data, including, during an interview with the employee, deleting copies of the files from a personal device and account where they were discovered. Although Rakuten does not have any indication of misuse of the data at this time, it cannot be certain what occurred once the data was outside of its environment or whether the data was transferred to or exists on any other accounts. Rakuten has been in touch with law enforcement and is continuing to work to ensure the security of this information.

The type of information impacted includes name, address, date of birth, and Social Security number.

Notice to New Hampshire Residents

On February 11, 2021, Rakuten began providing written notice of this incident to individuals whose information has been determined to have been in the impacted files based on the investigation to date, which includes nine (9) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

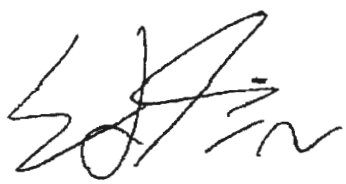
Upon discovering the event, Rakuten moved quickly to investigate and respond to the incident, assess the security of Rakuten systems, and notify potentially affected individuals. Rakuten is also working to implement additional safeguards and training to its employees. Rakuten is providing access to credit monitoring services for two (2) years, through Epiq, to letter recipients, at no cost to these individuals.

Additionally, Rakuten is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rakuten is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF:jcj
Enclosure

EXHIBIT A

Rakuten

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>:

Rakuten USA, Inc. DBA Rakuten Americas ("Rakuten") is writing to inform you of a recent data security event that involves some of your personal information. We take this event seriously and are providing you with information about the incident and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On or about January 21, 2021, Rakuten's data security team detected that an employee who was in the process of voluntarily leaving the company had transferred a number of files off their Rakuten-issued computer. As soon as we learned about this person's actions, we launched an investigation into the nature and scope of their activity. Our investigation revealed that some of these transferred files contained sensitive personal information of employees. This person had been authorized to access this information only on a Rakuten device for assigned work purposes. We immediately took steps to limit potential further exposure of the data, including, during an interview with the employee, deleting copies of the files from a personal device and account where they were discovered. Although we do not have any indication of misuse of the data at this time, we cannot be certain what occurred once the data was outside of our environment, including whether the data was further transferred or other copies were made. Rakuten has been in touch with law enforcement and is continuing to work to ensure the security of this information.

What Information Was Involved? The information involved includes your name, Social Security number and date of birth.

What We Are Doing in Response? The security of information in our care is among our highest priorities. Although we do not have any knowledge of actual or attempted misuse of the exposed information at this time, we are notifying you, so that you may take further steps to best protect yourself from potential harm. We are offering you access to complimentary credit monitoring, fraud consultation, and identity theft restoration services through TransUnion, in which you can enroll using the information on the attached pages. In addition, we are providing notice to appropriate regulatory authorities. Besides our investigation into this particular incident, we are reviewing our existing policies and procedures and will implement additional safeguards, as needed.

What Can You Do? As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity from threats arising from any source. You may also review the information contained in the attached "Steps You Can Take to Help Protect Your Information." There you will also find more information on the credit monitoring and identity protection services we are making available to you. While Rakuten will cover the cost of these services, you will need to complete the enrollment and activation process.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-978-2680, Monday through Friday, from 9 am to 9 pm Eastern Time. You may also write to us at 800 Concar Dr., San Mateo, CA 94402 Attn: Privacy.

Sincerely,

Adrienne Down Coulson
Chief Operating Officer, Rakuten Americas

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

See last page for credit monitoring instructions.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity for threats from any source. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	https://www.transunion.com/fraud-alerts	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov/.

For Washington, D.C. residents, the Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov/.

For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226; or 1-919-716-6400, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is one (1) Rhode Island resident impacted by this incident.

TransUnion

Activation Code: <<Activation Code>>

Complimentary Two-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static six- digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)