COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG
LONDON LOS ANGELES NEW YORK PALO ALTO
SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956

Via FedEx

May 19, 2023

New Hampshire Department of Justice
Attn: Security Breach Notification
33 Capitol St
Concord, NH 03301

Re: Legal Notice of Information Security Breach Pursuant to N.H. Rev. Stat. Ann. § 359-C:19 *et seq.*

To Whom It May Concern:

In accordance with the above-referenced provision of New Hampshire law, I write on behalf of Exeter Finance LLC ("Exeter") to inform you of an information security incident involving a third party, NCB Management Services, Inc. ("NCB"), and potentially affecting approximately three (3) residents of New Hampshire.

Exeter is an auto finance company that works with franchised and independent dealers nationwide to help consumers finance vehicle purchases. In connection with providing accounts receivable services for Exeter-owned accounts, NCB had been granted access to certain information from Exeter, including information about Exeter account holders.

On April 24, 2023, Exeter received notification from NCB that a cybersecurity incident on NCB's systems involved information from Exeter. Exeter understands from NCB that on or about February 4, 2023, NCB identified a cybersecurity incident involving unauthorized access by a third party to its systems on or about February 1, 2023. Based on the information available to date from NCB, Exeter understands that the incident involved access by an unauthorized party to information about Exeter account holders and co-borrowers.

NCB has informed Exeter that it has taken steps to eliminate the unauthorized activity on NCB's systems, and that it has notified and is cooperating with law enforcement. NCB has also informed Exeter that it has implemented additional security measures to harden its network and increase its ability to monitor and detect threats, as well as additional data security training of its workforce.

At this time, Exeter believes based on information from NCB that the data involved for Exeter account holders and co-borrowers included individuals'

Exeter also understands that NCB has not received any reports of misuse of this data.

NCB, in coordination with Exeter, has identified and will notify on Exeter's behalf approximately three (3) potentially affected individuals who are residents of New Hampshire. In addition, NCB will provide identity monitoring services to these individuals. Enclosed is a copy of the notification letter that NCB will send to potentially affected individuals via first-class mail on or about May 19, 2023.

The notification to individuals will include: (1) a description of the incident in general terms, including the approximate date of the incident and the types of personal information at issue; (2) the actions taken by NCB to protect personal information from further possible unauthorized access; (3) an address and a phone number to call for further information and assistance; (4) information on how the individual may enroll in free identity monitoring and other complimentary services arranged by NCB; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free phone number, address, and website for the Federal Trade Commission, and a statement that individuals can obtain information on identity theft from this source; and (8) advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports.

If you have any questions or need further information regarding this incident, please feel free to contact me.

Respectfully Submitted,

Caleb W. Skeath
Counsel to Exeter Finance LLC

NCB Management Services

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

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

<<b2b_text_1(Re: Notice of Data Breach)>>

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

We are writing to you about a recent security incident at NCB Management Services, Inc. ("NCB") which may have affected some of your personal information. NCB is a national accounts receivable management company that provides account services to companies. You are receiving this notice because we determined that your records are among those that were accessed without authorization.

Recently, confidential client account information maintained by NCB on behalf of its client, <<b2b_text_3(Business Partner Name)>>, was accessed by an unauthorized party. To date, we are unaware of any misuse of your information as a result of this incident. However, we are notifying you and providing tools you can use to help protect against possible identity theft or fraud, should you feel it is appropriate to do so.

WHAT HAPPENED: On February 4, 2023, NCB discovered that an unauthorized party gained access to NCB's systems on February 1, 2023. After a thorough investigation, NCB confirmed that some of your information was accessed by the unauthorized party and notified its client on <<b2b_text_4(Data Owner Notification Date)>> about the unauthorized access. NCB has obtained assurances that the unauthorized third party no longer has access to any of NCB's data.

WHAT INFORMATION WAS INVOLVED: The information involved may have included your . We are not aware of any use or distribution of the accessed information.

WHAT WE ARE DOING: We are notifying you so you can protect your personal and account information. After detecting unusual activity, we took immediate steps to identify and contain the intrusion and eliminate the unauthorized activity on NCB's systems. We have implemented a number of additional security measures to harden our network and increase our ability to monitor and detect any threats. We are also conducting additional training of our workforce on data security. NCB has notified and is cooperating with federal law enforcement authorities.

Although we have not received any reports of misuse of this information, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $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 deadline)>> to activate your identity monitoring services.
Membership Number: <<Membership Number s_n>>

NCB Management Services

For more information about Kroll and your identity monitoring services, you can visit www.info.krollmonitoring.com.

Additional information describing these services is included with this letter. Please note that you must activate to take advantage of this free service, and we encourage you to do so.

WHAT YOU CAN DO: In addition to activating the complimentary services offered, we recommend you review your credit reports and account statements over the next 12 to 24 months and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft. Refer to the enclosed "Important Additional Information" for other precautions you can take.

FOR MORE INFORMATION: If you have any questions about this incident, please contact , Monday – Friday between 9:00 a.m. and 6:30 p.m. Eastern Time, excluding major U.S. holidays.

We regret the concern or inconvenience this incident may cause you.

Sincerely,

NCB

ENC: Important Additional Information

Important Additional Information

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

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

For residents of *New Mexico*: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights pursuant to the federal Fair Credit Reporting Act. Please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General
400 6th Street NW
Washington, D.C. 20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

Rhode Island Office of Attorney General
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

For residents of Massachusetts and Rhode Island: You have the right to file or obtain a police report if you are a victim of identity theft. There were approximately 3,500 Rhode Island residents notified by NCB on behalf of itself and its business partners in connection with this incident.

For Residents of New York: You may contact the Federal Trade Commission, the New York Attorney General or the State Department Division of Consumer Protection about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

New York Attorney General
120 Broadway
3rd Floor
New York, NY 10271
800-771-7755
www.ag.ny.gov

New York State Department Division of Consumer Protection
One Commerce Plaza
99 Washington Ave
Albany, NY 12231-0001
800-697-1220
https://dos.ny.gov/consumer-protection

For residents of all states:

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze for yourself or your spouse or a minor under 16: (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; (5) proof of current address, such as current utility or telephone bill, bank, or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. However, fees may apply to other services offered by the consumer reporting agencies.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/
888-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
https://www.experian.com/help/
888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-help
800-916-8800

You may also contact the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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.

$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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and 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.