

EXHIBIT 1

Our office continues to represent Roadrunner Transportation Systems, Inc. (“RRTS”), 1431 Opus Place, Suite 530, Downers Grove, IL 60515. We write to supplement our September 10, 2018 notice to your office (“September 10 Notice”), a copy of which is attached as ***Exhibit A***. By providing this supplemental notice, RRTS does not waive any rights or defenses regarding the applicability of California law, applicability of the California data event notification statute, or personal jurisdiction.

Since providing the initial notice, RRTS identified 463 additional affected residents of California. Notice to those individuals was mailed on October 9, 2018, after RRTS confirmed the individuals’ mailing addresses, in substantially the same form as ***Exhibit A*** of the September 10 Notice.

RRTS is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, RRTS is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one’s credit file, 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.

EXHIBIT A



XAVIER BECERRA

Attorney General

Search

[Translate Website](#) | [Traducir Sitio Web](#)

Create Data Breach Report (SB24)

[Home](#) / [Privacy](#) / [Create Data Breach Report \(SB24\)](#)

The answer you entered for the CAPTCHA was not correct.

This submission is required by California Civil Code s. 1798.29(e); California Civil Code s. 1798.82(f)

Note: This form is only for use by businesses and state and local government agencies, which are required to submit a sample notice if they experience a breach of personal information involving more than 500 California residents.




If you are a consumer who wishes to file a complaint, please use our online complaint form.

SECTION 1 - ATTACH SECURITY BREACH NOTIFICATION SAMPLE

Sample of Notice

California Civil Code s. 1798.29(e) and s. 1798.82(f) provide that "A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code." A copy of this notification will be made available online.

Click browse button to select file and then click upload to attach the file.

File information	Display	Operations
 RRTS - July 2018 - Notice of Data Event - CA - Exhibit 1.pdf 315.26 KB		 Remove
<div>Description</div>		

SECTION 2 - INFORMATION FOR LAW ENFORCEMENT PURPOSES

The information provided in SECTION 2 is for DOJ use.

Organization Name

Roadrunner Transportation Systems, Inc.

Address

1431 Opus Place, Suite 530

City

Downers Grove

State

Illinois▼

Zip Code

60515

Date(s) of Breach (if known)

I'm not a robot

reCAPTCHA
Privacy - Terms

Date(s) of Breach (if known)

Date

2018-04-01

E.g., 2018-09-10

Date(s) of Breach (if known) 2

Date

2018-04-29

E.g., 2018-09-10

Add another Date

Date(s) of Discovery of Breach

Date(s) of Discovery of Breach

Date

2018-07-02

E.g., 2018-09-10

Add another Date

Date(s) Individual Notice Provided to Consumers

Date(s) Individual Notice Provided to Consumers

Date

2018-09-10

E.g., 2018-09-10

Add another Date

Was notification delayed because of a law enforcement investigation?

- ☐ N/A
- ☒ No
- ☐ Yes

Type of Personal Information Involved in the Breach

- None -
Social Security Number Information
Driver's License number or California ID Card number information
Financial Information (e.g. account number, credit or debit card numbers)

Brief Description of the Breach

See Exhibit 1.

Report Type

- ☐ N/A
- ☐ Addendum to Previous Report
- ☒ Initial Breach Report

Breach Affecting

- ☐ N/A
- ☐ Fewer Than 500 Individuals
- ☒ 500 or More Individuals

Approximate Number of Individuals Affected by the Breach

9821

Approximate Number of Californians Affected by the Breach

937

Type of Entity

- None -
BSO - Businesses - Other
BSF - Businesses - Financial and Insurance Services
BSR - Businesses - Retail or Merchant
EDU - Educational Institutions

Is the organization a small business, according to the Small Business Administration? *

- ☐ Yes
- ☒ No
- ☐ Unsure

(See the Small Business Administration's standards for defining a "small business": www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf.)

Type of Breach

- ☐ Unintended disclosure
- ☐ Hacking or malware
- ☐ Payment Card Fraud
- ☐ Insider
- ☐ Physical loss
- ☐ Portable device
- ☐ Stationary device
- ☒ Other

If Type of Breach is "Other" please describe the type of breach here

Phishing

Location of Breached Information

E-mail ▼

If Location of Breached Information is "Other" please describe the location here

Was Substitute Notice Given?

- ☐ N/A
- ☐ No
- ☒ Yes

Was Media Notice Given?

- ☐ N/A
- ☐ No
- ☒ Yes

Name of company contact whom the Attorney General may contact for further information

Jim Prendergast, Mullen Coughlin LLC

Telephone Number

267-930-4798

Email address

jprendergast@mullen.law

Was a law enforcement agency notified regarding the breach?

- ☐ N/A
- ☒ No
- ☐ Yes

If Yes, name of law enforcement agency and contact name and number

Was a police report filed?

- ☐ N/A
- ☒ No
- ☐ Yes

If yes, police report number

Submit form

[Submit](#)

eCrime

[eCrime Unit](#)[High Technology Theft Apprehension and Prosecution \(HTTAP\) Program](#)[Investigations & Guidelines](#)[File a Complaint](#)

Data Security Breach (SB24)

[Data Security Breach Reporting](#)[Submit Data Security Breach](#)[Search Data Security Breaches](#)

Related Information

[2016 Data Breach Report, pdf](#)[Breach Help: Tips For Consumers](#)[Cybersafety](#)[Data Breach Statistics, pdf](#)[eCrime](#)[Identity Theft](#)[Privacy](#)

SB24 Administration

[All Submitted Data Security Breaches](#)[Published Data Security Breaches](#)[Pending Review of Data Security Breaches](#)[Rejected Data Security Breaches](#)

Data Security Breach (SB24)

[Data Security Breach Reporting](#)

[Submit Data Security Breach](#)

[Search Data Security Breaches](#)

Related Information

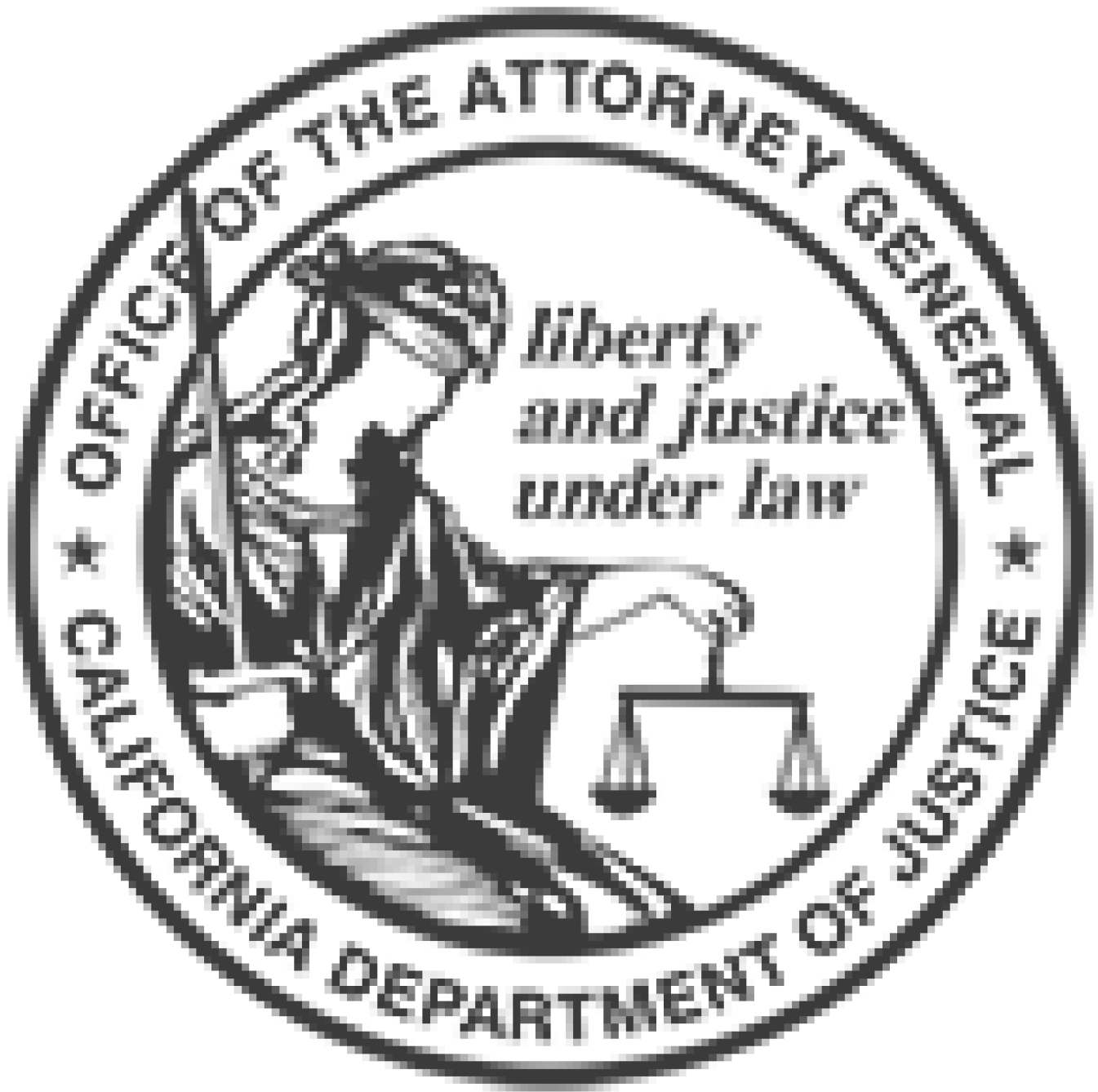
[Communication Service Providers Legal Process Information](#)

[Cybersafety](#)

[Data Security Breach Reporting](#)

[Internet Crime Complaint Center](#)

[Money Wiring Scams](#)



**STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL**

<input type="text"/>	Search
----------------------	--------

WHO WE ARE

[About AG Xavier Becerra](#)

[History of the Office](#)

[Organization of the Office](#)

WHAT WE DO

Public Safety
Opinions and Quo Warranto
Research
Children & Families
Civil Rights
Consumer Protection
Environment & Public Health
Tobacco Directory
Tobacco Grants

OPEN GOVERNMENT

Ballot Initiatives
Conflicts of Interest
Criminal Justice Statistics
Meetings and Public Notices
OpenJustice Initiative
Public Records
Publications
Regulations

Memorial

Agents Fallen in the Line of Duty

Vote

Register to Vote

WHAT WE'RE WORKING ON

21st Century Policing
Children's Rights
Consumer Protection and Economic Opportunity
Environmental Justice
Equality
Health Care
Immigration
OpenJustice

MEDIA

Consumer Alerts
Press Releases
Media Library

CAREERS

Getting a State Job
Examinations
Job Vacancies
Internships & Student Positions

Attorney General's Honors Program

Earl Warren Solicitor General Fellowship

[Office of the Attorney General](#)

[Accessibility](#)

[Privacy Policy](#)

[Conditions of Use](#)

[Disclaimer](#)

[© 2018 DOJ](#)

**XAVIER BECERRA***Attorney General*

Search

[Translate Website](#) | [Traducir Sitio Web](#)

Data Breach Submission Confirmation

[Home](#) / [Privacy](#) / [Submit Data Security Breach](#) / [Data Breach Submission Confirmation](#)

Data Breach Report (SB24) *Submitted Breach Notification Sample* has been created.



On behalf of the Office of the Attorney General, I would like to thank you for your submission.

eCrime

[eCrime Unit](#)[High Technology Theft Apprehension and Prosecution \(HTTAP\) Program](#)[Investigations & Guidelines](#)[File a Complaint](#)

Data Security Breach (SB24)

Data Security Breach Reporting

Submit Data Security Breach

Search Data Security Breaches

Related Information

2016 Data Breach Report, pdf

Breach Help: Tips For Consumers

Cybersafety

Data Breach Statistics, pdf

eCrime

Identity Theft

Privacy

Related Information

Communication Service Providers Legal Process Information

Cybersafety

Data Security Breach Reporting

Internet Crime Complaint Center

Money Wiring Scams



**STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL**

WHO WE ARE

About AG Xavier Becerra

History of the Office

Organization of the Office

WHAT WE DO

Public Safety

Opinions and Quo Warranto

Research

Children & Families

Civil Rights

Consumer Protection

Environment & Public Health

Tobacco Directory

Tobacco Grants

OPEN GOVERNMENT

Ballot Initiatives

Conflicts of Interest

Criminal Justice Statistics

Meetings and Public Notices

OpenJustice Initiative

Public Records

Publications

Regulations

Memorial

Agents Fallen in the Line of Duty

Vote

Register to Vote

WHAT WE'RE WORKING ON

21st Century Policing

Children's Rights

Consumer Protection and Economic Opportunity

Environmental Justice

Equality

Health Care

Immigration

[OpenJustice](#)

MEDIA

[Consumer Alerts](#)

[Press Releases](#)

[Media Library](#)

CAREERS

[Getting a State Job](#)

[Examinations](#)

[Job Vacancies](#)

[Internships & Student Positions](#)

[Attorney General's Honors Program](#)

[Earl Warren Solicitor General Fellowship](#)

[Office of the Attorney General](#)

[Accessibility](#)

[Privacy Policy](#)

[Conditions of Use](#)

[Disclaimer](#)

© 2018 DOJ

EXHIBIT 1

The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Roadrunner Transportation Systems, Inc. ("RRTS") does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

Nature of the Data Event

On July 2, 2018, RRTS became aware that they were the subject of a phishing campaign attack and that several employees had inadvertently clicked on the phishing email. RRTS immediately commenced an investigation into this activity to determine what happened and what information may be affected. This investigation included working with third party forensic investigators to confirm the nature and scope of this incident. Through the investigation, we determined that there was unauthorized access to several employee email accounts in April 2018. It is believed that this access occurred after the employees received phishing emails. On August 13, 2018, the results of the data mining of those accounts was completed and the affected population was identified. The investigation determined that the personal information accessible in the email accounts included credit/debit card number and credit/debit card security code or password, driver's license number, financial account number, medical information, health insurance information, Social Security Number and State Identification Number.

Notice to California Residents

RRTS provided written notice to potentially affected individuals by mail on or about September 10, 2018 which includes nine hundred and thirty-seven (937) California residents. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and to Be Taken

Upon discovering the incident, RRTS moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident. RRTS is providing all potentially affected individuals complimentary access to twelve (12) free months of credit and identity monitoring services, including identity restoration services, through Kroll. Additionally, RRTS is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. RRTS is also providing written notice of this incident to other state regulators as necessary.

EXHIBIT A



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We write regarding a recent email phishing event that may have impacted the security of your personal information. We want to provide you with information about the incident, our response and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On July 2, 2018, Roadrunner Transportation Systems, Inc. ("RRTS") became aware that they were the subject of a phishing campaign attack and that several employees had inadvertently clicked on the phishing email. RRTS immediately commenced an investigation into this activity to determine what happened and what information may be affected. This investigation included working with third party forensic investigators to confirm the nature and scope of this incident. Through the investigation, we determined that there was unauthorized access to several employee email accounts in April 2018. It is believed that this access occurred after the employees received phishing emails. On August 13, 2018, the results of the data mining of those accounts was completed and the affected population was identified.

What Information was Involved? A review of the email accounts determined that information related to you was contained therein that may have been viewed without authorization. This information included your <<ClientDef1>><<ClientDef2>> (name, address, [data elements]).

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Upon learning of the event, we immediately commenced an investigation to confirm the nature and scope of the incident and to identify what information may be affected. We also took steps to prevent further unauthorized access to the email accounts by changing passwords. While we have measures in place to protect information in our systems, we are reviewing our existing policies and procedures.

As an added precaution, we are offering you access to twelve months (12) of identity monitoring services to include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration services through Kroll at no cost to you. Please review the attached "Steps You Can Take to Protect Your Information" for information on these services and instruction on how to activate services. We encourage you to activate these services as we are not able to act on your behalf to do so.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information," which contains information on what you can do to better protect against possible misuse of your information. You may also activate the identity monitoring services we are offering. In addition, we encourage you to routinely change your passwords to your accounts to avoid unauthorized access.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact 1-833-228-5713, Monday through Friday from 9:00 am to 6:00 pm Eastern Standard Time, excluding U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read 'CStoelting', with a stylized, cursive script.

Curt Stoelting
Chief Executive Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Activate Your Identity Monitoring Services

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

You have until **November 29, 2018** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5713. Additional information describing your services is included with this letter.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports and explanation of benefits forms for suspicious activity. 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 listed below to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice was not delayed as the result of a law enforcement investigation.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716- 6400; and online at www.ncdoj.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 violator. 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.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.