



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED
JUL 31 2020
CONSUMER PROTECTION

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

July 27, 2020

INTENDED FOR ADDRESSEE(S) ONLY

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 Select Express & Logistics (“Select”) located at 55 W 39th St, 15th floor, New York, NY 10018, and write, on behalf of Select, to notify your Office of an incident that may affect the security of certain personal information of approximately four (4) New Hampshire residents. The investigation into this event is ongoing, and this notice may be supplemented if significant facts learned subsequent to its submission. By providing this notice, Select does not waive any rights or defenses regarding the applicability of New Hampshire law, the New Hampshire data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On May 3, 2020, Select learned of suspicious activity impacting the operability of certain Select systems. Select immediately launched an investigation to determine the nature and scope of this activity. Working with third-party forensic investigators, Select determined that an unknown actor encrypted certain systems using malware, and also used malware to acquire a small number of files from Select’s server. In addition, the investigation produced evidence of unauthorized access to a limited number of Select employee email accounts from February 7, 2020 to May 5, 2020. For some of these accounts, the investigation was unable to determine if any specific email or attachment was actually viewed. Select, therefore, undertook a review of the contents of the email accounts and acquired files that could have been impacted. Through this review, which was completed on July 8, 2020, it was determined personal information was present in the affected email accounts or the files that may have been acquired by the malware. The investigation determined that the following types of information related to New Hampshire residents may have been accessible within the impacted accounts: name and Social Security number.

Notice to New Hampshire Residents

On or around July 27, 2020, Select began providing written notice of this incident to potentially affected individuals, including approximately four (4) 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

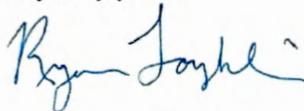
Upon learning of unusual activity in its system, Select immediately took steps to secure the affected accounts and acquired files and launched an in-depth investigation, with the assistance of a third-party forensic investigation firm, to determine the nature and scope of this incident. As part of Select's ongoing commitment to the privacy of personal information in its care, Select is reviewing its existing policies and procedures and implementing additional safeguards to further secure the information in its systems. Select notified law enforcement and is also notifying relevant regulatory authorities of this event, as required by applicable law.

Additionally, Select is providing potentially impacted individuals with complimentary access to identity monitoring, fraud consultation, and identity theft restoration services through Kroll. Select is providing potentially affected 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/crm
Enclosure

EXHIBIT A



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

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

Re: Notice of Data Breach

Dear <<FirstName>> <<LastName>>:

Select Express & Logistics ("Select") is writing to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, Select's response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On May 3, 2020, Select learned of suspicious activity impacting the operability of certain Select systems. Select immediately launched an investigation to determine the nature and scope of this activity. Working with third-party forensic investigators, Select determined that an unknown actor encrypted certain systems using malware, and also used malware to acquire a small number of files from Select's server. In addition, the investigation produced evidence of unauthorized access to a limited number of Select employee email accounts from February 7, 2020 to May 5, 2020. For some of these accounts, the investigation was unable to determine if any specific email or attachment was actually viewed. Select, therefore, undertook a review of the contents of the email accounts and acquired files that could have been impacted. Through this review, which was completed on July 8, 2020, it was determined that some of your personal information was present in the affected email accounts or the files that may have been acquired by the malware.

What Information Was Involved? The information potentially acquired included your <<b2b_text_1(ImpactedData)>>. To date, Select is unaware of any actual or attempted misuse of your personal information as a result of this incident.

What We Are Doing. Select takes this incident and the security of personal information in its care seriously. Upon learning of this incident, Select moved quickly to investigate and respond, assess the security of relevant Select systems, and identify potentially affected individuals. As part of Select's ongoing commitment to the security of information, Select is also reviewing existing policies, procedures, and security measures. Select notified law enforcement of this event and is reporting this event to relevant state regulators.

Select is offering you access to complimentary identity monitoring services for twelve (12) months through Kroll. If you wish to activate the identity monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. 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. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the identity monitoring, fraud consultation, and identity theft restoration services Select is making available to you. While Select will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-844-954-2388 (toll free), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding U.S. holidays). You may also write to Select at: 55 W 39th St, 15th floor, New York, NY 10018.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kern Weissman', written in a cursive style.

Kern Weissman
Chief Information Officer
Select Express & Logistics

Steps You Can Take to Help Protect Personal Information

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for twelve (12) months. 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, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **October 30, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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 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

PO Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

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

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

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, 1-410-528-8662, www.oag.state.md.us.

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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, 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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There are 6 Rhode Island residents impacted by this incident.](#)

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; <https://ag.ny.gov/>.



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.

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.