



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 11 2020

CONSUMER PROTECTION

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienzo@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 4, 2020

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 Peregrine Corporation d/b/a PSL Services ("PSL Services") located at 39 Darling Ave., South Portland, ME 04106, and are writing to notify your office of an incident that may affect the security of some personal information relating to certain New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PSL Services 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 December 17, 2019, PSL Services discovered suspicious activity in an employee's email account. PSL Services immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic specialist, it was determined that a number of PSL Services' employees' email accounts were subject to unauthorized access for periods of time between December 16, 2019 and December 19, 2019. PSL Services undertook a time-consuming review of the contents of the email accounts that were accessed to determine if they contain sensitive information. This review and the identification of potentially affected individuals was completed on March 13, 2020. The information that could have been subject to unauthorized access includes name, address, date of birth, Social Security number, Driver's license number, financial account/routing number, medical and diagnostic treatment information, and health insurance information. PSL Services then

continued to research addresses for the affected individuals in order to provide direct notice to the affected individuals.

Notice to New Hampshire Residents

On or about May 4, 2020, PSL Services began providing written notice of this incident to affected individuals, which includes sixteen (16) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. PSL Services is also providing notice of this incident on its website. A copy of the website notice is attached here as *Exhibit B*.

Other Steps Taken and To Be Taken

Upon discovering the event, PSL Services moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. PSL Services is also working to implement additional safeguards and training to its employees. PSL Services is offering potentially impacted individuals with access to credit monitoring services at no cost to the individuals.

Additionally, PSL Services 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. PSL Services 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. PSL Services is also providing notice of this incident to any regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,



Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:plm
Enclosure(s)

EXHIBIT A

Peregrine Corp, DBA PSL Services

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Event

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Peregrine Corporation d/b/a PSL Services ("PSL Services") is writing to advise you of an incident that may affect the security of some of your personal information. We take this incident very seriously and are providing you with information and access to resources so you can better protect against the possibility of the misuse of your personal information should you feel it is appropriate to do so.

What Happened? On December 17, 2019, PSL Services discovered suspicious activity in an employee's email account. PSL Services immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that a number of PSL Services' employees' email accounts were subject to unauthorized access for periods of time between December 16, 2019 and December 19, 2019. Thereafter, PSL Services undertook a time-consuming review of the contents of the email accounts that were accessed to determine if they contain sensitive information.

What Information Was Involved? The information in the email accounts that was potentially subject to unauthorized access includes your: <<ClientDef1(ImpactedData)>>.

What We Are Doing. PSL Services takes this incident and the security of information in its care very seriously. PSL Services reviewed its existing security measures and implemented additional safeguards to prevent similar incidents from occurring in the future. PSL Services also notified the Office of Civil Rights at the Department of Health and Human Services and any required state or federal regulators regarding this incident.

As an added precaution, PSL Services is offering you access to 24 months of complimentary identity monitoring and identity theft consultation and restoration services through Kroll. The cost of this service will be paid for by PSL Services. Instructions on how to activate the identity monitoring services can be found in the enclosed Steps You Can Take to Help Protect Against Identity Theft and Fraud.

What Can You Do? As a best practice, you should always carefully review your Explanations of Benefits forms for suspicious or unauthorized activity and report any instances of fraud to law enforcement. You can also review the attached "Steps You Can Take to Help Protect Against Identity Theft and Fraud" for more information regarding how to further safeguard your personal information should you feel it appropriate to do so.

For More Information. We understand that you may have questions about the incident that are not addressed in this letter. If you have additional questions, or need assistance, please call 844-904-0954, Monday through Friday, from 9:00 am to 6:30 pm Eastern Time.

The security of personal information in our possession is a top priority. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Lori Sanville

Lori Sanville
Executive Director
Peregrine Corporation d/b/a PSL Services

Steps You Can Take to Help Protect Against Identity Theft and Fraud

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 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, Fraud Consultation, and Identity Theft Restoration.

Visit [https://\[IDMonitoringURL\]](https://[IDMonitoringURL]) to activate and take advantage of your identity monitoring services.

You have until [\[Date\]](#) to activate your identity monitoring services.

Membership Number: <<Member ID>>

Monitor Your Accounts. PSL Services encourages you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your 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 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:

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

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;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

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:

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should 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 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/>.

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 2 Rhode Island residents impacted by this incident.](#)

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 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.

EXHIBIT B

Peregrine Corporation d/b/a PSL Services Provides Notice of Data Security Incident

On May 4, 2020, Peregrine Corporation d/b/a PSL Services (“PSL Services”) announced that a recent event may have impacted the security of personal information related to certain individuals. PSL Services is providing notice of the incident on its website so individuals may take precautions to better protect against the possibility of the misuse of their personal information should they feel it is appropriate to do so.

What Happened? On December 17, 2019, PSL Services discovered suspicious activity in an employee’s email account. PSL Services immediately launched an investigation into the nature and scope of the incident. As part of the investigation, which was conducted with the assistance of a third-party forensic expert, it was determined that a number of PSL Services’ employees’ email accounts were subject to unauthorized access for periods of time between December 16, 2019 and December 19, 2019. Thereafter, PSL Services undertook a time-consuming review of the contents of the email accounts that were accessed to determine if they contain sensitive information.

What Information Was Involved? The information in the email accounts that was potentially subject to unauthorized access includes: name, address, date of birth, Social Security number, Driver’s license number, financial account/routing number, credit/debit card number, username/password, medical and diagnostic treatment information, health insurance information, EIS number and Maine Care number.

What We Are Doing. PSL Services takes this incident and the security of information in its care very seriously. PSL Services reviewed its existing security measures and implemented additional safeguards to prevent similar incidents from occurring in the future. PSL Services also notified the Office of Civil Rights at the Department of Health and Human Services and any required state regulators regarding this incident. PSL Services also notified prominent news media outlets throughout the state of Maine.

What Can You Do? As a best practice, you should always carefully review your Explanations of Benefits forms for suspicious or unauthorized activity and report any instances of fraud to law enforcement. You can also review the attached “Steps You Can Take to Protect Against Identity Theft and Fraud” for more information regarding how to further protect yourself should you feel it appropriate to do so.

For More Information. We understand that you may have questions about the incident that are not addressed here. If you have additional questions, or need assistance, please call 844-904-0954, Monday through Friday, from 9:00 am to 6:30 pm Eastern Time.

Steps You Can Take to Protect Against Identity Theft and Fraud

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

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872

www.transunion.com/credit-freeze

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

Equifax

P.O. 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;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

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:

TransUnion

P.O. Box 2000

Chester, PA 19106

1-800-680-7289

[www.transunion.com/fraud-victim-](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

[resource/place-fraud-](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

[alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

[alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Experian

P.O. Box 2002

Allen, TX 75013

1-888-397-3742

[www.experian.com/fraud/center.](http://www.experian.com/fraud/center.html)

[html](http://www.experian.com/fraud/center.html)

[html](http://www.experian.com/fraud/center.html)

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

[www.equifax.com/personal/cre](http://www.equifax.com/personal/credit-report-services)

[dit-report-services](http://www.equifax.com/personal/credit-report-services)

[dit-report-services](http://www.equifax.com/personal/credit-report-services)

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.