



BOARD OF GOVERNORS *of the*
COLORADO STATE UNIVERSITY SYSTEM

OFFICE OF THE GENERAL COUNSEL

01 Administration Building • 0006 Campus Delivery
Fort Collins, Colorado 80523-0006
Phone: (970) 491-6270 • Fax: (970) 491-2118

August 16, 2023

Office of Consumer Protection

DELIVERED VIA E-MAIL: ocpdatabreach@mt.gov

Re: Notice of Security Event

To whom it may concern,

Our office represents The Board of Governors of the Colorado State University System and its various campuses and affiliated entities including, Colorado State University, Colorado State University – Pueblo, and Colorado State University – Global (hereinafter “CSU”), on all legal matters.

In accordance with Mont. Code § 30-14-1701 et seq., CSU is providing the following notice as expeditiously as practicable disclosing a security event affecting CSU’s institutional data. By providing notice, CSU does not waive any rights or defenses regarding the applicability of Montana law, the applicability of the Montana data notification statute, or personal jurisdiction.

On July 10, 2023, our office received notice of a possible security event affecting our institutional data through one of CSU’s vendors, the National Student Clearinghouse (“NSC”). An investigation was immediately launched to determine the scope and effect of the disclosed security event.

Nature of the Security Event

On or around May 31, 2023, Progress Software Corporation publicly disclosed zero-day vulnerabilities that impacted its MOVEit Transfer software (“MOVEit”). MOVEit is a secure file transfer software utilized by many companies around the world, including Pension Benefits Information, LLC (“PBI”) and the National Student Clearinghouse (“NSC”) in their day-to-day operations for the handling of sensitive information.

After NSC notified CSU that it was impacted by the MOVEit vulnerability, CSU initiated its investigative efforts. The initial investigation quickly determined that no CSU’s systems or data infrastructure had been affected. However, additional vendors affected by the security event who were holding institutional data on behalf of CSU were identified (“Identified Vendors”). As with CSU, the Identified Vendors’ systems were not personally affected. Identified Vendors were affected through their individual business relationship with PBI.

The investigation revealed that Clop, a well-known Russian threat actor, exploited the disclosed vulnerability, accessed PBI and NSC’s MOVEit Transfer servers, and exfiltrated certain data from those servers, which included information related to residents of Montana. The information that could have been subject to unauthorized access includes first name, last name, Social Security number, or some combination of the above.

On Monday, August 14, 2023, CSU concluded its scope investigation in coordination with the Identified Vendors and NSC. No individuals whose personal information was held by NSC on behalf of CSU were affected. However, a total of 19,344 individuals whose personal information was held by the Identified Vendors on behalf of CSU were affected, including 92 residents of the state of Montana.

Notice

The individual notification process has begun and will continue on a rolling basis. A sample copy of the written notice is attached hereto as **Exhibit A**.

Other Steps Taken and To Be Taken

Upon discovering the security event, CSU moved quickly to investigate the security event, confirm that no CSU systems were impacted, and identify potentially affected individuals. While the investigation was ongoing, CSU issued a notice to its community members to provide as much information as possible and provide guidance on how to better protect against identity theft and fraud via a website available at https://csusystem.edu/moveit_cyberattack/. CSU and its vendors are reviewing their policies, procedures, and cybersecurity safeguards to further protect their systems. CSU will continue to work with the Identified Vendors to ensure notice is provided to the affected individuals in accordance with the law. CSU is providing written notice of this security event to relevant state regulators, as necessary.

PBI and NSC promptly began applying available patching, which was first available June 2, 2023, and undertaking the recommended mitigation steps. Additionally, both companies notified relevant law enforcement agencies and, with the assistance of third-party cybersecurity specialists, launched internal investigations to determine the potential impact of the vulnerabilities' presence on their MOVEit Transfer servers and the data housed within. Based on the results of their investigation, PBI and NSC notified the consumer reporting agencies, Equifax, Experian, and TransUnion. PBI and NSC are providing access to credit monitoring and identity theft restoration services, through Kroll, for two (2) years to individuals whose personal information was potentially affected by this security event, at no cost to these individuals. In addition, both PBI and NSC have established a toll-free call center for notified individuals to address any questions they may have related to the security event.

Contact Information

If you have any additional questions, you may reach out to the undersigned via email at mario.arango@colostate.edu or via telephone call at (970) 491-6920, at your convenience.

Respectfully,



Mario Arango
Associate Legal Counsel
The Colorado State University System

Exhibit A



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Date>>

<<City>>, <<State>> <<Zip>>

<<Country>>

<<Notice of Data Breach>>

Dear <<Name 1>> <<Name 2>>:

Pension Benefit Information, LLC (“PBI”) provides audit and address research services for insurance companies, pension funds, and other organizations<< , including <<Data Owner>>. PBI is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability’s impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: name and <<Data Elements>>.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to <<12/24>> months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and to report suspected identity theft incidents to the institution. Please also review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

For More Information. If you have additional questions, you may call our toll-free assistance line at <<Kroll Call Center Number>> Monday through Friday from 9:00 am to 6:30 pm Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<12/24>> 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.¹

Visit <<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>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **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 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);

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.

2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

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

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately [X] Rhode Island residents that may be impacted by this event.