



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

August 11, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Colorado Department of Health Care Policy & Financing (“HCPF”) located at 1570 Grant Street, Denver, Colorado 80203, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately seven hundred twenty-six (726) 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, HCPF 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 May 31, 2023, Progress Software discovered a problem affecting its MOVEit® Transfer application. IBM, a third-party vendor contracted with HCPF, uses the MOVEit application to move HCPF data files in the normal course of business. Progress Software publicly announced that the MOVEit problem was the result of a cybersecurity incident, which impacted many users around the world, including IBM. No HCPF or State of Colorado systems were affected by this issue.

After IBM notified HCPF that it was impacted by the MOVEit incident, HCPF launched an investigation right away to understand whether the incident impacted its own systems, and to determine whether Health First Colorado or CHP+ members’ protected health information was accessed by an unauthorized party. While HCPF confirmed that no other HCPF systems or databases were impacted, on June 13, 2023, the investigation identified that certain HCPF files on the MOVEit application used by IBM were accessed by the unauthorized actor on or about May 28, 2023. These files contained certain Health First Colorado and CHP+ members’ information.

The information that could have been subject to unauthorized access includes

Notice to New Hampshire Residents

On or about August 11, 2023, HCPF began providing written notice of this incident to approximately seven hundred twenty-six (726) 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 discovering the event, HCPF moved quickly to investigate the incident, confirm that no HCPF systems were impacted, and identify potentially affected individuals. HCPF and its vendors are reviewing their policies, procedures and cybersecurity safeguards to further protect their systems. HCPF is providing access to credit monitoring services for _____, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HCPF is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HCPF is providing individuals with 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.

HCPF is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. HCPF is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at _____.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/kzf
Enclosure

EXHIBIT A



COLORADO
Department of Health Care
Policy & Financing

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 11, 2023

J8481-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Dear Sample A. Sample:

We are writing to let you know about a recent incident that involves your personal information and/or protected health information. Our agency, the Department of Health Care Policy and Financing (HCPF), oversees Health First Colorado (Colorado's Medicaid program), Child Health Plan *Plus* (CHP+), and other health care programs for Coloradans who qualify.

What Happened? On May 31, 2023, Progress Software discovered a problem affecting its MOVEit® Transfer application. IBM, a third-party vendor contracted with HCPF, uses the MOVEit application to move HCPF data files in the normal course of business. Progress Software publicly announced that the MOVEit problem was the result of a cybersecurity incident, which impacted many users around the world, including IBM. No HCPF or State of Colorado systems were affected by this issue.

After IBM notified HCPF that it was impacted by the MOVEit incident, HCPF launched an investigation right away to understand whether the incident impacted our own systems, and to determine whether Health First Colorado or CHP+ members' protected health information was accessed by an unauthorized party. While we confirmed that no other HCPF systems or databases were impacted, on June 13, 2023, the investigation identified that certain HCPF files on the MOVEit application used by IBM were accessed by the unauthorized actor on or about May 28, 2023. These files contained certain Health First Colorado and CHP+ members' information. We have since learned that some of your information was included in these files. Pursuant to state law and the Health Insurance Portability and Accountability Act (HIPAA), we are required to give you notice of this breach.

What Information Was Involved? The information may have included one or more of the following pieces of information: your

What We Are Doing. We take information security seriously and apologize for any inconvenience this incident may cause. HCPF and its vendors are reviewing their policies, procedures and cybersecurity safeguards to further protect their systems. As an added precaution, we are offering you of free credit monitoring and identity restoration services provided through Experian. Unfortunately, HCPF cannot enroll you directly due to privacy reasons. So if you would like to enroll, please read *Steps You Can Take to Protect Personal Information* included with this letter. We have also set up a call center to answer additional questions you may have. Please call us at , Monday through Friday, 7:00 a.m. to 9:00 p.m. Mountain Time, or Saturday and Sunday, 9:00 a.m. to 6:00 p.m. Mountain Time (excluding major holidays). Please be prepared to provide engagement number

What You Can Do. We encourage you to remain vigilant against identity theft and fraud by reviewing your bank and credit card accounts and monitoring your free credit reports to detect suspicious activity and errors. You may also review *Steps You Can Take to Protect Personal Information*, which we have included with this letter.

Sincerely,

Jane Wilson

Jane Wilson
Privacy Officer
www.hcpf.colorado.gov/MOVEit-cyber-security

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering a complimentary membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
- Provide your **activation code:**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at by November 30, 2023. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Monitor Your Accounts

Under U.S. law, you are 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. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

You have the right to place an initial or extended fraud alert on your credit file at no cost.

- If your information has **not** been used for identity theft, you can ask for an initial fraud alert. This alert will be placed in your credit file and lasts for one year. If you have an initial fraud alert in your credit file, businesses must take steps to verify your identity before they approve new credit. This can help stop identity thieves from taking out new credit cards and loans in your name.
- If your information has been used for identity theft, you are entitled to an extended fraud alert, which lasts seven years. If you want to place an extended fraud alert, please contact any of the three major credit reporting bureaus listed below.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, be aware that using a credit freeze to take control over who gets access to your personal and financial information 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. Under federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you 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.);
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 you are a victim of identity theft.

If you want to place a credit freeze or fraud alert on your credit file, you will need to contact **each** of 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

Learn more about identity theft, fraud alerts, credit freezes, and steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. Please file a complaint with the Federal Trade Commission if your information has been misused. Contact the Federal Trade Commission if you have questions about how to file your complaint.

You also have the right to file a police report if you ever experience identity theft or fraud. To file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Contact your local police department if you have questions about the type of proof you will need.

Instances of known or suspected identity theft should also be reported to your state Attorney General.

Residents of states OTHER than Colorado, please read the following:

For California residents, 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; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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. There are 301 Rhode Island residents that may be impacted by this event.

Help in your Language

Please Call: 833-346-1583

Español	ATENCIÓN: Si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística.
Tiếng Việt	CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn.
繁體中文	注意：如果您使用繁體中文，您可以免費獲得語言援助服務。
한국어	주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다.
Русский	ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода.
አማርኛ	ማሳሰቢያ: የሚናገሩት ቋንቋ አማርኛ ከሆነ የትርጉም እርዳታ ድርጅቶች በነጻ ሊያግዝዎት ተዘጋጅተዋል፡
العربية	ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان.
Deutsch	ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung.
Français	ATTENTION: Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement.
नेपाली	ध्यान दिनुहोस्: तपाईंले नेपाली बोल्नुहुन्छ भने तपाईंको निम्ति भाषा सहायता सेवाहरू निःशुल्क रूपमा उपलब्ध छ ।
Tagalog	PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad.
日本語	注意事項：日本語を話される場合、無料の言語支援をご利用いただけます。
Oroomiffa	XIYYEEFFANNAA: Afaan dubbattu Oroomiffa, tajaajila gargaarsa afaanii, kanfaltiidhaan ala, ni argama.
فارسی	توجه: اگر به زبان فارسی گفتگو می کنید، تسهیلات زبانی بصورت رایگان برای شما فراهم می باشد.
Polski	UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej.