UnitedHealthcare Privacy Office
185 Asylum Street
CT950-1000
Hartford, CT 06103

Via Email Only

July 28, 2023

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

RE: Privacy Breach Notification
UHC File #: 623174

Dear Attorney General:

I am writing to inform you of a recent security incident affecting UnitedHealthcare Student Resources ("Student Resources," "we," or "our") that impacted Iowa residents.

On May 31, 2023, Progress Software announced it discovered a previously unknown ("zero-day") vulnerability in its MOVEit Transfer and Cloud based software that could allow an authorized third party to access files sent with the software. Immediately upon discovering this, Student Resources began investigating and took action to patch the vulnerabilities. On June 12, 2023, we discovered that the threat actor had successfully exploited the MOVEit vulnerability on May 27, 2023, four (4) days before the zero-day vulnerability was announced. On June 28, 2023, we determined that the exploitation led to the unauthorized access of information for Eight hundred twenty-six (826) Iowa residents.

This exploitation of the MOVEit vulnerability resulted in disclosure of individuals' information. While the information varied by individual, it may have included a combination of: name, date of birth, address, phone number, email address, plan identification number, policy information, student identification number, Social Security number or national identification number, and claims information, including claim numbers, provider information, dates of service, diagnosis codes, prescription information, and claims financial information. This incident did not involve the disclosure of driver's license number, or any financial account information.

As soon as Student Resources was made aware of the MOVEit zero-day vulnerability, it took steps to isolate its server and applied all patches as soon as they were released. Further, the MOVEit server was not brought back online until after an investigation

confirmed there was no persistent threat, and additional safeguards could be put in place such as credential rotation, blocking of HTTP/HTTPS traffic, additional logging, and additional firewall restrictions.

Student Resources takes matters such as this very seriously. A sample of the notification letter being sent to impacted individuals is enclosed herewith. Affected individuals will be provided steps they can take to protect their identities, including informing them that they should report suspected incidents of identity theft to local law enforcement or the attorney general. The notice letter will also explain how to place a fraud alert and/or security freeze on affected individuals' credit files and provide them with the contact information for the national credit reporting agencies and the Federal Trade Commission.

Student Resources maintains an information security program and has put additional protections in place to prevent such incidents from occurring in the future, including reinforcing our existing policies and practices, and evaluating additional safeguards.

If you have any questions about this incident, please contact me directly.

Sincerely,

Chris R. Nelson, CIPP/US, CIPP/E
Staff Attorney
UnitedHealthcare Corporate
860-702-5042
chris_r_nelson@Student Resources.com

185 Asylum Street | CT950-1000| Hartford, Connecticut 06103

UnitedHealthcare Privacy Office
Attn: Chris Nelson
PO Box 1459
Minneapolis MN 55440

Notice of Data Breach

[Date]

[Name]
[Address Line 1]
[Address Line 2]
[City, STATE, Zip code]

Dear [Name],

We are writing to let you know about a privacy issue involving some of your information.

What Happened?

On May 31, 2023, Progress Software, announced it discovered a previously unknown ("zero-day") vulnerability in the MOVEit software that could allow an unauthorized third party to access files sent with the software. Upon learning of the vulnerability, UnitedHealthcare Student Resources ("Student Resources" or "we") immediately began investigating the use of the MOVEit software and any potential impact. On June 1, 2023, we discovered suspicious activity on a Student Resources file transfer server and confirmed exploitation of the vulnerability on June 12, 2023. *MOVEit Transfer* servers are used by organizations and governments around the world to send and receive data. On June 28, 2023, we determined that your information was impacted as a result of the incident. We believe this incident occurred on May 27, 2023.

What Information Was Involved?

The information involved may have included your: name, date of birth, address, phone number, email address, plan identification number, policy information, student identification number, Social Security number or national identification number, and claim information, including claim numbers, provider information, dates of service, diagnosis codes, prescription information, and financial information associated with claims. This incident did not involve disclosure of your driver's license number or any financial account information.

What We Are Doing

Upon discovery, we took prompt action to investigate the matter. Student Resources took the MOVEit server offline until additional protections could be put in place, including the installation of new software patches developed to eliminate the vulnerability and blocked certain types of traffic to the server. Additionally, we notified law enforcement of the incident.

What You Can Do

You can sign up for the free identity theft protection service that we have provided. Please check your explanation of benefits statements, bills and accounts to be sure they look correct. We have attached steps on how to do that. We have also attached instructions on how to help protect your information as well as contact the U.S. Federal Trade Commission, place an alert or freeze on your Credit File, or contact your state attorney general if applicable.

We suggest that you retain this notice for your records.

For More Information

Student Resources takes this matter very seriously and is committed to protecting the privacy and security of our plan participants' information.

If you have any questions or concerns, please call us toll-free at 866-341-4262, Monday through Friday between 7am – 7pm CST.

We deeply regret any inconvenience or concern caused by this incident.

Sincerely,

Chris R. Nelson
Staff Counsel
UnitedHealthcare Privacy Office

U.S. Citizens:

NortonLifeLock Identity Theft Protection Enrollment Instructions

UnitedHealth Group has partnered with **NortonLifeLock** to offer you two years of complimentary **LifeLock Standard™** identity theft protection. Your Promo Code is [redacted] and your Member ID is [redacted]. You have until **November 17, 2023**, to enroll in this service at no cost to you.

To activate your membership online and get protection at no cost to you:

1. Go to LifeLock.com
2. Locate the promo code box below the protection plan boxes. Enter [redacted] and click 'Apply.'
3. Your complimentary offer is presented. Click the START MEMBERSHIP button.
4. A popup will prompt you to enter your Member ID. Enter it and click APPLY.
5. Once enrollment is completed, you will receive a confirmation email. Be sure to follow all directions in this email.

If you prefer to activate your membership by phone, please call: 1-800-861-2023.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Standard™**[1] membership includes:

✓LifeLock Identity Alert™ System†
✓ 24/7 Live Member Support
✓ Dark Web Monitoring**
✓ LifeLock Privacy Monitor™
✓ Lost Wallet Protection
✓ Stolen Funds Reimbursement up to $25,000 †††
✓ Personal Expense Compensation up to $25,000 †††
✓ Coverage for Lawyers and Experts up to $1 million †††
✓ U.S.-Based Identity Restoration Team
✓ One-Bureau Credit Monitoring[1]**
✓ Reduced Pre-Approved Credit Card Offers
✓ USPS Address Change Verification

1 If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features:
(i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
** These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Standard. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Non-U.S. Citizens:

NortonLifeLock Identity Theft Protection Enrollment Instructions

UnitedHealth Group has retained **NortonLifeLock** to provide Two 2 years of complimentary **Norton 360 Deluxe™** identity theft protection. Your Promo Code is [redacted] and your Member ID is [redacted].

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to Norton.com/UHC
2. Click on "Enter Promo Code" on the right side of the screen and enter the promo code above.
3. Enter your Member ID in the popup window and click "APPLY."
3. Please start your enrollment process and once enrollment is completed, you will receive a confirmation email (be sure to follow ALL directions in this email).

Alternatively, to activate your membership over the phone, please call: **1-800-861-2023**.

You will have until **November 17, 2023**, to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **Norton 360 Deluxe™** membership includes:

- ✓ Real-Time Threat Protection for your Device
- ✓ Dark Web Monitoring**
- ✓ Secure VPN
- ✓ Password Manager
- ✓ Privacy Monitoring

[1]Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, and Android devices. Norton account features are not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.
**These features are not enabled upon enrollment. Members must take action to get their protection.

Reference Guide

1. Review Your Account Statements

Remain vigilant for incidents of potential fraud and identity theft. Carefully review account statements and credit reports to make sure that all of your account activity is valid. Report any questionable charges promptly to the financial institution or company with which you maintain the account.

As a precaution to protect against misuse of your health information, we recommend that you remain vigilant and regularly monitor the explanation of benefits statements that you receive from your plan, and your bank and credit card statements, credit reports, and tax returns to check for any unfamiliar activity. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please contact your plan. If you do not regularly receive explanation of benefits statements, you may request that your plan send you these statements following the provision of any health care services in your name or plan number by contacting your plan at the number on your member ID card. If you notice any suspicious activity on either your bank or credit card statement, or tax returns, please immediately contact your financial institution and/or credit card company, or relevant institution.

2. Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

Upon receiving your credit report, review them carefully. Look for any accounts you did not open. Look in the "inquires" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for inaccuracies in information (such as home address and Social Security number).

If you see anything that you do not understand, call the credit bureau at the telephone number of the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

3. Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
1-866-653-4261 (TTY)
https://consumer.ftc.gov/features/identity-theft

4. Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be a victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging your file with a fraud alert at all three bureaus.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	P.O. Box 105069 Atlanta, GA 30348-5069	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

5. Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file, at no cost to you, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) phone number, current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

You can request a security freeze for free by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-800-916-8800	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about security breach response and steps you can take to help prevent identify theft. Please see the information below for states that provide these resources:

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office
Director of Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Phone: 1-515-281-5926
Website: www.iowattorneygeneral.gov

For Maryland Residents. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place

25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For Residents of Massachusetts. You have the right to obtain a police report with respect to this incident. 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: New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For New York Residents. You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General
The Capitol

Albany, NY 12224-0341

Phone: 1-800-771-7755
Website: www.ag.ny.gov

For North Carolina Residents. You can obtain information about preventing and avoiding identity theft from the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000
Website: https://ncdoj.gov/
Identity Theft Link: https://ncdoj.gov/protecting-consumers/protecting-your-identity/

For Oregon Residents. State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Department of Justice at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301

Phone: 1-877-877-9392
Website: www.doj.state.or.us

For Rhode Island Residents. You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

Phone: 1-401-274-4400
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#

Help You Avoid Becoming a Victim

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues, or any other internal information. If an unknown, individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, https://www.cisa.gov/news-events/news/protecting-your-privacy).

5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (https://apwg.org/).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls for Home and Small Office Use, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, https://www.cisa.gov/news-events/news/understanding-anti-virus-software; and Reducing Spam, https://www.cisa.gov/news-events/news/reducing-spam).

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.