

## Appendix

We are writing on behalf of The Johns Hopkins University (“JHU”) and The Johns Hopkins Health System Corporation (“JHHS”) (collectively “Johns Hopkins”), regarding a data security incident involving Maine residents. Johns Hopkins is also providing this notice on behalf of Kennedy Krieger Institute, to which it provides services.

On May 31, 2023, Johns Hopkins was notified by a third-party software vendor, Progress Software, of a zero-day vulnerability in its commercial file transfer software, MOVEit. Johns Hopkins took immediate action, including disconnecting the Johns Hopkins server that utilizes the MOVEit software and engaging a third-party cybersecurity incident response team to assist with forensic analysis and ongoing monitoring. The investigation determined that an unauthorized party had exploited the vulnerability and gained access to the Johns Hopkins server that hosted the MOVEit software on May 29, 2023, and was able to download documents off of this server.

Johns Hopkins conducted a comprehensive review of the involved documents to identify individuals whose information was included. Based on this review, Johns Hopkins determined that the documents included certain Maine residents’ information. The information involved varied by individual, but may have included their name and Social Security number. All other systems at Johns Hopkins operate independently from the MOVEit server and were not impacted by this incident, and no data was lost or deleted. Johns Hopkins’ systems have remained fully operational throughout this incident and there has been no impact to student classes, patient care or services.

On June 23, 2023, Johns Hopkins began mailing notification letters to affected individuals, which includes a total of 43 Maine residents, via U.S. First-Class Mail in accordance with Me. Rev. Stat. Tit. 10, §1348. A breakdown of the number of Maine residents notified per entity is enclosed as **Attachment A**. A sample copy of the notification letter is enclosed as **Attachment B**. Johns Hopkins is offering affected individuals two-years of complimentary credit monitoring and identity protection services, and has also established a dedicated, toll-free call center where individuals may obtain more information regarding the incident.

Johns Hopkins is committed to maintaining the privacy and security of the personal information it maintains and is taking this incident very seriously. To help prevent something like this from happening in the future, Johns Hopkins has implemented the recommended patching and remediation steps to secure its MOVEit server and will continue to look for ways to enhance its secure file transfer protocols.

**Attachment A**

<b>Notifying Entity</b>	<b>Number of Maine Residents</b>
<b>JHU</b>	34
<b>JHHS</b>	8
<b>KENNEDY KRIEGER INSTITUTE</b>	1

# Attachment B



Return to IDX  
P.O. Box 989728  
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

**Privacy Office**  
Johns Hopkins Health System  
Johns Hopkins University  
733 N. Broadway, MRB  
Suite 102B  
Baltimore, MD 21205

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 11, 2023

Re: Compromise of Information

Dear <<First Name>> <<Last Name>>:

We are writing to notify you about a cybersecurity incident that involved some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident, the measures we are taking in response, and offer steps you may consider taking.

### What Happened?

On May 31, 2023, Johns Hopkins was notified by a third-party software vendor, MOVEit, of a technical vulnerability in its software. We took immediate action, including disconnecting the Johns Hopkins server that utilizes the MOVEit software and engaging a third-party cybersecurity incident response team to assist with forensic analysis and ongoing monitoring. The investigation determined that an unauthorized party had gained access to the Johns Hopkins server that hosted the MOVEit software on May 29, 2023, and was able to download documents off of this server containing Johns Hopkins information. This cybersecurity incident also impacted many other providers and businesses nationally and internationally.

### What Information Was Involved?

The information downloaded included your <<Data Element>>. The incident did not impact Johns Hopkins electronic medical records and no information was lost or deleted.

### What We Are Doing

Johns Hopkins is committed to maintaining the privacy and security of your information and is taking this incident very seriously. We have been working with our business partners and law enforcement to mitigate this situation as best as possible.

Additionally, to assist in protecting you from any potential identity theft, we are providing you with two years of credit monitoring and resolution services through IDX, A ZeroFox Company, the data breach and recovery services expert. You can enroll by calling (888) 703-9247 or going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. Please note the deadline to enroll is September 13, 2023.

IDX identity protection services include: two years of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

**What You Can Do**

We recommend you monitor your accounts and watch for any suspicious activity. If you suspect or discover that your information has been used inappropriately, please notify your local law enforcement or consumer protection agency. For more information on additional steps you can take to protect your information, please see the pages that follow this letter.

**For More Information**

Please visit [www.HopkinsMedicine.org/DataAttack](http://www.HopkinsMedicine.org/DataAttack) for more information about this incident. If you have any additional questions, please do not hesitate to contact IDX at (888) 703-9247 on weekdays between the hours of 9 am and 9 pm ET.

All of us at Johns Hopkins sincerely regret any concern this incident may cause.

Sincerely,

*Carol M. Richardson*

Carol M. Richardson  
Chief Privacy Officer

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

If your payment card information was involved, we remind you to remain vigilant to the possibility of fraud by reviewing your card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card network rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the pages that follow this notice for additional steps you may take.

### ***Fraud Alerts and Credit or Security Freezes:***

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

***Additional information for residents of the following states:***

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us).

**Massachusetts:** Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection> | *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**Rhode Island:** This incident involves 33 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.





Return to IDX  
 P.O. Box 989728  
 West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>  
 <<Address1>>  
 <<Address2>>  
 <<City>>, <<State>> <<Zip>>

IT@JH Office of CIO  
 Johns Hopkins University and John Hopkins Medicine  
 5801 Smith Avenue  
 Davis Building, Suite 3110B  
 Baltimore, MD 21209

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:

Or Visit:  
<https://app.idx.us/account-creation/protect>

July 11, 2023

Re: Compromise of Information

Dear <<First Name>> <<Last Name>>:

We are writing to notify you about a cybersecurity incident that involved some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident, the measures we are taking in response, and offer steps you may consider taking.

**What Happened?**

On May 31, 2023, Johns Hopkins was notified by a third-party software vendor, MOVEit, of a technical vulnerability in its software. We took immediate action, including disconnecting the Johns Hopkins server that utilizes the MOVEit software and engaging a third-party cybersecurity incident response team to assist with forensic analysis and ongoing monitoring. The investigation determined that an unauthorized party had gained access to the Johns Hopkins server that hosted the MOVEit software on May 29, 2023, and was able to download documents off of this server containing Johns Hopkins information. This cybersecurity incident also impacted many other providers and businesses nationally and internationally.

**What Information Was Involved?**

The information downloaded included your <<Data Element>>. We have confirmed that no information was lost or deleted.

**What We Are Doing**

Johns Hopkins is committed to maintaining the privacy and security of your information and is taking this incident very seriously. We have been working with our business partners and law enforcement to mitigate this situation as best as possible.

Additionally, to assist in protecting you from any potential identity theft, we are providing you with two years of credit monitoring and resolution services through IDX, A ZeroFox Company, the data breach and recovery services expert. You can enroll by calling (888) 703-9247 or going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above.

IDX identity protection services include: two years of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note the deadline to enroll is September 13, 2023.



**What You Can Do**

We recommend you monitor your accounts and watch for any suspicious activity. If you suspect or discover that your information has been used inappropriately, please notify your local law enforcement or consumer protection agency. For more information on additional steps you can take to protect your information, please see the pages that follow this letter.

**For More Information**

Please visit <http://www.jhu.edu/DataAttack> for more information about this incident. If you have any additional questions, please do not hesitate to contact IDX at (888) 703-9247 on weekdays between the hours of 9 am and 9 pm ET.

All of us at Johns Hopkins sincerely regret any concern this incident may cause.

Sincerely,

A handwritten signature in black ink, appearing to read 'R Mendola', with a long horizontal flourish extending to the right.

Richard A. Mendola  
Vice President and Chief Information Officer

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111  
*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

If your payment card information was involved, we remind you to remain vigilant to the possibility of fraud by reviewing your card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card network rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the pages that follow this notice for additional steps you may take.

### ***Fraud Alerts and Credit or Security Freezes:***

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)  
**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

***Additional information for residents of the following states:***

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us).

**Massachusetts:** Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection> | *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**Rhode Island:** This incident involves 10 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You must be told if information in your file has been used against you.

You have the right to know what is in your file.

You have the right to ask for a credit score.

You have the right to dispute incomplete or inaccurate information.

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 reports to be provided to employers.

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.

You have a 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.

You may seek damages from violators.

Identity theft victims and active duty military personnel have additional rights.