

January 30, 2024

VIA U.S. MAIL

Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Hematologics, Inc. – Incident Notification

Dear Mr. Frey:

McDonald Hopkins PLC represents Hematologics, Inc. (“Hematologics”). I am writing to provide notification of an incident at Hematologics that may affect the security of personal information of approximately one (1) resident. Hematologics investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Hematologics does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

Hematologics received notice from one of its third-party vendors, Paycor, Inc. (“Paycor”), regarding a security vulnerability in the MOVEit Transfer solution which is utilized by Paycor. There was no compromise of Hematologics network security. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on MOVEit Transfer. MOVEit has acknowledged the vulnerability and, as of June 2, 2023, provided patches to remediate the exploit. Upon being informed of the vulnerability, Paycor immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third party professionals to assist in the investigation and remediation of the vulnerability. The analysis showed that the incident’s scope was limited to the third party MOVEit Transfer platform.

After their investigation, Paycor notified Hematologics on November 30, 2023 that certain files that contain personal information belonging to Hematologics were potentially removed from the Paycor network by an unauthorized party on or around May 31, 2023. Following Hematologics review of the information and data provided by Paycor, Hematologics discovered on December 6, 2023, which Hematologics files were impacted by the incident. The impacted data includes full name, address, Social Security Number, and health insurance information. Not all data elements were impacted for every Maine resident. On January 29, 2024, Hematologics located the most recent contact information for the impacted individuals.

January 30, 2024

Page 2

To date, Hematologics is not aware of incidents of financial fraud or identity fraud as a result of the incident. Nevertheless, out of an abundance of caution, Hematologics is providing notice to the affected clients commencing on January 30, 2024, in substantially the same form as the enclosed letter (Attached as Exhibit A). All notified individuals will receive complimentary credit monitoring services. Furthermore, Hematologics will advise all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Hematologics will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for Hematologics. Hematologics remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Hematologics continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (410) 917 5189 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock

Encl.

Exhibit A



January 30, 2024

Dear

The privacy and security of the personal information entrusted to us is of the utmost importance to Hematologies, Inc. (“Hematologies”). We are writing to provide you with information regarding a recent incident which involves the security of some of your personal information. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, let you know that there is no indication of any compromise within the Hematologies environment and that we continue to take significant measures to protect your information.

What Happened?

Hematologies received notice from one of our third-party vendors, Paycor, Inc. (“Paycor”), regarding a security vulnerability in the MOVEit Transfer solution which is utilized by Paycor. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on MOVEit Transfer. MOVEit has acknowledged the vulnerability and, as of June 2, 2023, provided patches to remediate the exploit. **Furthermore, there was no compromise of Hematologies network security.**

What We Are Doing.

Upon being informed of the vulnerability, Paycor immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third party professionals to assist in the investigation and remediation of the vulnerability. The analysis showed that the incident’s scope was limited to the third party MOVEit Transfer platform. After their investigation, Paycor notified Hematologies on November 30, 2023 that certain files that contain personal information belonging to Hematologies were potentially removed from the Paycor network by an unauthorized party on or around May 31, 2023. Following our review of the information and data provided by Paycor, we discovered on December 6, 2023 which Hematologies files were impacted by the incident.

What Information Was Involved?

The information that may have been accessed contained some of your personal information, including your



What You Can Do.

We have no evidence that any of your information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and to help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [REDACTED]

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by May 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [REDACTED]
- Provide your **activation code**: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by May 31, 2024. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

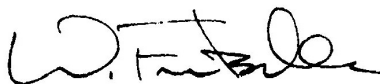
This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are disappointed, of course, that Hematologics valued employees have been involved and inconvenienced by this third-party data security incident. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We stress that there is no indication of any compromise within the Hematologics environment. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available [REDACTED]

Sincerely,



Wayne Fritschle, Chief Operating Officer
Hematologics, Inc.
3161 Elliott Ave
Suite 200
Seattle, WA 98121

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring
ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** 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.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. State Specific Resources.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.