MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James Cope
Office: (267) 930-4766
Fax: (267) 930-4771
Email: JCope@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 9, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent OneBlood, Inc. ("OneBlood") located at 8669 Commodity Circle, Orlando, FL 32819, and are writing to notify your office of an event that may affect the security of certain information relating to 1,049 Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, OneBlood does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around July 28, 2024, OneBlood became aware of suspicious activity within its network. It began an investigation to determine the full nature and scope of the event. This investigation determined that between July 14 to July 29, 2024, certain files and folders were copied from its network without authorization. OneBlood promptly conducted a comprehensive review of the affected files to identify the types of information contained in them and to whom the information relates. On or about December 12, 2024, it completed this review and quickly worked to identify complete contact information for potentially affected individuals. On December 23, 2024, OneBlood completed the additional review and determined that the affected files contained the information for 1,049 Maryland residents.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maryland Residents

On or about January 9, 2025, OneBlood provided written notice of this event to 1,049 Maryland 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 becoming aware of the event, OneBlood moved quickly to investigate and respond to the event, assess the security of OneBlood systems, and identify potentially affected individuals. Further, OneBlood notified federal law enforcement regarding the event. OneBlood is providing access to credit monitoring services for twelve (12) months, through Transunion, to notified individuals at no cost to these individuals.

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

OneBlood is providing written notice of this event to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4766.

Very truly yours,

James Cope of
MULLEN COUGHLIN LLC

JC1/kzs
Enclosure

EXHIBIT A

OneBlood, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

oneblood

[redacted]

000010102G0500

P

January 9, 2025

Dear [redacted]:

OneBlood, Inc. ("OneBlood") is providing notice of an event that involves some of your information. We take this event very seriously and are providing details of the event and information on the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around July 28, 2024, OneBlood became aware of suspicious activity within its network. We began an investigation to determine the full nature and scope of the event. Our investigation determined that between July 14 to July 29, 2024, certain files and folders were copied from our network without authorization. We conducted a comprehensive review of the affected files to identify the types of information contained in them and to whom the information relates. On or about December 12, 2024, we completed our review and determined that the affected files contained your information.

What Information Was Involved? The investigation determined that your name and Social Security number was included in the relevant files and folders.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. In response to this event, we promptly took steps to secure our systems and conducted a detailed investigation to confirm the full nature and scope of the event. We also notified federal law enforcement of this event.

As an added precaution, we are also offering you complimentary access to twelve (12) months of credit monitoring and identity theft restoration services, through TransUnion. Please review the instructions in the attached *Steps You Can Take to Help Protect Your Personal Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against instances of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the provided information on steps you can take to protect personal information and to enroll in the identity protection services by following the instruction in the *Steps You Can Take to Protect Your Personal Information* section below.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call at [redacted], Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. You may also write to OneBlood at Oneblood, Inc., Attention: TransUnion, 8669 Commodity Circle, Orlando, FL 32819

Sincerely,

OneBlood, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary credit monitoring services being offered to you by logging on to https://bfs.cyberscout.com/activate and following the provided instructions. When prompted, please provide the following unique code: [redacted]. To receive the monitoring services, please enroll within 90 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

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

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

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

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

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

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; 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 approximately <<#>> Rhode Island residents that may be impacted by this event.

P 0000102028000