



---

## Notice of Data Security Incident

**Paducah, KY. February 25, 2025** – Merryman House Domestic Crisis Center (“MHDCC”), a service provider dedicated to supporting individuals affected by domestic violence, is providing notice of a recent data security incident that may have resulted in the unauthorized access to certain individuals’ personal information. This notice is intended to share information about the incident, steps MHDCC is taking in response to the incident, and resources Merryman is providing to help protect those impacted against the potential misuse of their information.

**What Happened?** On or around June 12, 2024, MHDCC detected suspicious activity on its computer systems. Upon discovery of this incident, MHDCC immediately secured its systems and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. The forensics investigation determined that certain client data contained in MHDCC’s systems was accessed by an unauthorized actor. If you received services from Merryman between 2015 and 2024, your information may have been exposed.

**What Information Was Involved?** Although MHDCC has no evidence that any sensitive information has been misused by third parties as a result of this incident, MHDCC is providing this notice out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information may have been subject to unauthorized access: name, address, social security number, driver license or state ID number, or financial information.

**What Are We Doing?** Data privacy and security is among MHDCC’s highest priorities, and MHDCC is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the incident, MHDCC moved quickly to investigate, respond, and confirm the security of its systems. In addition, MHDCC has taken the following steps since the incident: adopted encryption technologies, enforced password changes and a 60-day rotation policy, implemented new technical safeguards including MFA on O365/VPN accounts, and implemented periodic technical and non-technical evaluations. The server/data backups were upgraded to a more secure device with a high level of protection, and offsite storage points. End User Training for Cyber security was implemented for all staff.

In light of the incident, MHDCC is providing resources to those impacted. For adults, MHDCC is providing access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. For minors, MHDCC is providing Dark Web Monitoring services at no charge. These services will provide alerts for 12 months from the date of enrollment when changes occur to an individual’s credit file. A notification is sent the same day that the change or update takes place with the bureau. Finally, MHDCC is providing proactive fraud assistance to help with any questions or in event that an individual becomes a victim of fraud. These services will be provided by Transunion, specializing in fraud assistance and remediation services. While we are covering the cost of these services, individuals will need to complete the activation process by following the instructions below.



**What Can You Do to Protect Your Data?** If you or someone you know received domestic violence services at MHDCC, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Resources To Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

**How to enroll for the free services?** To enroll in Credit Monitoring or Dark Web Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services:

- CYAIBDULN12MHDCC – Adult Credit Monitoring 12 months
- FMAYCMH11SKUW7 – Minor Cyber Monitoring 12 months

In order for you to receive the monitoring services described above, you must 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 under the age of 18 years of age. 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.

We encourage you to take full advantage of the services offered.

### **Other Important Information**

Should you have any questions or concerns, please call 1-833-799-3770 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

MHDCC remains dedicated to ensuring the privacy and security of all information in our control and sincerely apologizes for any inconvenience.

Sincerely,

**MERRYMAN HOUSE DOMESTIC CRISIS CENTER**



## **ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION**

### **Monitor Your Accounts**

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

### **Credit Freeze**

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

### **Fraud Alert**

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not



block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

### Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

### Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
<b>Experian</b>	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 <a href="http://www.experian.com">www.experian.com</a>	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 <a href="https://www.experian.com/fraud/center.html">https://www.experian.com/fraud/center.html</a>	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>
<b>Equifax</b>	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 <a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 <a href="http://www.equifax.com/personal/credit-report-services/credit-fraud-alerts">www.equifax.com/personal/credit-report-services/credit-fraud-alerts</a>	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
<b>TransUnion</b>	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 <a href="http://www.transunion.com">www.transunion.com</a>	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com/fraud-alerts">www.transunion.com/fraud-alerts</a>	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>



**Iowa and Oregon residents** are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

**Massachusetts residents** are advised of their right to obtain a police report in connection with this incident.

**District of Columbia residents** are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6<sup>th</sup> St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at [consumer.protection@dc.gov](mailto:consumer.protection@dc.gov).

**Maryland residents** can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

**New York residents** are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/) or <https://www.identitytheft.gov/#/>.

**North Carolina residents** are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting [www.ncdoj.gov](http://www.ncdoj.gov), or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

**Rhode Island residents** are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.