

RECEIVED

DEC 29 2025

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

R. David Lane, Esq.
Direct Dial: 248.402.4072
E-mail: dlane@mcdonaldhopkins.com

CONSUMER PROTECTION

December 24, 2025

VIA U.S. MAIL

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Unity Hunt, Inc. – Incident Notification

To Whom it May Concern:

McDonald Hopkins PLC represents Unity Hunt, Inc. (“Unity Hunt”). I am writing to provide notification of an incident at Unity Hunt that may affect the security of personal information of one (1) New Hampshire resident. By providing this notice, Unity Hunt does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Unity Hunt learned that an unauthorized party gained access to certain Unity Hunt systems from approximately March 7, 2025 to approximately March 13, 2025. Upon learning of this issue, Unity Hunt immediately launched an investigation and contained and secured the network. As part of the investigation, Unity Hunt worked very closely with third-party cybersecurity professionals experienced in handling these types of incidents to secure the environment and to identify the scope of what personal information, if any, was involved.

Following a comprehensive investigation and manual document review, Unity Hunt concluded on or about September 23, 2025, that one or more of the files or folders accessed and/or acquired by the unauthorized party as a result of this incident contained certain personal information pertaining to particular individuals. The personal information contained within the impacted data, as it relates to New Hampshire residents, included the first and last name and Social Security number.

Unity Hunt has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, Unity Hunt wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Unity Hunt is providing the affected resident with notification of this incident, commencing on or about December 24, 2025. The notice will be in substantially the same form as the letter attached hereto. Unity Hunt is also offering the affected resident whose Social Security number was determined to be impacted a complimentary membership with a credit

December 24, 2025

Page 2

monitoring service. Unity Hunt is advising the affected resident to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. Unity Hunt is also advising the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected resident is being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Unity Hunt, protecting the privacy of personal information is a top priority. Unity Hunt is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Unity Hunt continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (248) 402-4072 or email me at dlane@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in cursive script, appearing to read "R. David Lane".

R. David Lane, Esq.

Encl. Notice Letter



UNITY HUNT, INC.

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

[Redacted]

[Redacted]

[Redacted]

Dear [Redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Unity Hunt, Inc. ("Unity Hunt"). We are writing with important information regarding a data security incident that may have impacted some of your information. As such, we want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Unity Hunt learned that an unauthorized party gained access to certain Unity Hunt systems from approximately March 7, 2025, to approximately March 13, 2025.

What Unity Hunt Is Doing.

Upon learning of this issue, Unity Hunt immediately launched an investigation and contained and secured the network. As part of the investigation, Unity Hunt worked very closely with third-party cybersecurity professionals experienced in handling these types of incidents to secure the environment and to identify the scope of what personal information, if any, was involved. After a thorough forensic investigation and manual document review, on September 23, 2025, we confirmed that the potentially impacted data may have included a limited amount of your personal information.

What Information Was Involved?

The data involved contained certain personal information related to you, including your full name and [Redacted]

What You Can Do.

To date, we are not aware of any reports of identity fraud or identity theft, or any other misuse of personal information as a direct result of this incident. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident. To protect you from the potential misuse of your information, we are offering you a complimentary [Redacted] month membership of Epiq - Privacy Solutions ID credit monitoring. For more information on identity theft prevention and the credit-monitoring product being offered to you, including instructions on how to activate your complimentary [Redacted] month membership, please see the additional information provided below in this letter in the section labeled, "Other Important Information."

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or 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. Also, you can consider contacting your financial institution to request additional fraud protection and alerts on your accounts.

For More Information.

Please accept our apologies that this incident occurred. Unity Hunt is committed to maintaining the privacy of personal information in our possession and has taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of personal information. If you have any further questions regarding this incident, please call [REDACTED] between the hours [REDACTED] pm Eastern Time, Monday through Friday (excluding holidays).

Sincerely,

Unity Hunt, Inc.

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring.

To help protect your identity, we are offering complimentary access to Epiq - Privacy Solutions ID for [REDACTED] months.



Activation Code: [REDACTED]
Enrollment Deadline: [REDACTED]
Coverage Length: [REDACTED] Months

Epiq - Privacy Solutions ID
1B Credit Monitoring - Plus

How To Enroll:

1. Visit [REDACTED] and click "Activate Account"
2. Enter the following activation code, [REDACTED] and complete the enrollment form
3. Complete the identity verification process
4. You will receive a separate email from [REDACTED] confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5. Enter your log-in credentials
6. You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report¹

1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring

Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring

Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection

3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to \$1M Identity Theft Insurance²

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT²

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at [REDACTED] Monday-Friday [REDACTED] p.m., ET.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year “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 anyone (1) of the three (3) 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 charge. 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 contacting all three (3) nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three (3) credit reporting companies:

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 (1) free credit report every twelve (12) months from each of the above three (3) 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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, 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 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.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

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.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400.

As noted above, 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 have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

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, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request in writing from a consumer to temporarily lift a freeze on a credit report must comply with the request no later than three (3) business days after receiving the request. If the request is made online or by phone, the consumer reporting agency must comply with the request within one (1) hour.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

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 have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.


