



A business advisory and advocacy law firm®

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

August 17, 2022

VIA U.S. MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Newcourse Communications, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Newcourse Communications, Inc. (“Newcourse Communications”), which provides mailing services to financial institutions, including Old National Bank. I am writing to provide notification of an incident at Newcourse Communications that may affect the security of personal information of approximately 23 Maryland residents. As a Newcourse Communications client, Old National Bank provided personal information to Newcourse Communications for mailing services purposes and Newcourse Communications collected and processed personal information on Old National Bank’s behalf. Newcourse Communications’ 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, Newcourse Communications and Old National Bank do not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Newcourse Communications recently discovered that unauthorized access to its network occurred between April 27, 2022, and May 3, 2022. Upon learning of this incident, Newcourse Communications immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on its network. Based on its ongoing comprehensive investigation and document review, Newcourse Communications discovered on August 5, 2022 that a limited amount of personal information was exposed as a result of this incident. The type of personal information exposed varied but may have included the affected residents’ full names, addresses, Social Security numbers and loan numbers.

To date, Newcourse Communications is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Newcourse Communications wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075



residents against identity fraud. Newcourse Communications is providing the affected residents with written notification of this incident commencing on or about August 18, 2022 in substantially the same form as the letter attached hereto. Newcourse Communications is offering the affected residents complimentary two-year memberships with a credit monitoring service. Newcourse Communications is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being advised to contact their financial institution to inquire about steps to take to protect their loan accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General.

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

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Colin M. Battersby', with a stylized, flowing script.

Colin M. Battersby

Encl.



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

To Enroll, Please Call:

1-833-764-2927

Or Visit:

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

Enrollment Code: [REDACTED]

***NOTICE OF DATA BREACH
PLEASE REVIEW CAREFULLY***

August 18, 2022

Dear [REDACTED]

We are writing with important information about a recent security incident. The privacy and security of the information we maintain is of the utmost importance to Newcourse Communications, Inc., which provides mailing services to financial institutions including Old National Bank. The purpose of this letter is to:

- Provide you with information about the incident.
- Explain the free services we are making available to you.
- Assure you that we continue to take significant measures to protect your information.

What Happened?

We recently discovered that unauthorized access to our network occurred between April 27, 2022, and May 3, 2022. Upon learning of this incident, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network.

What Information Was Involved?

Based on our ongoing comprehensive investigation and document review, we discovered on August 5, 2022 that your personal information was exposed as a result of this incident. The type of personal information exposed varied but may have included [REDACTED].

What We Are Doing

While we are not currently aware of any reports of identity fraud or improper use of your information as a result of this incident, out of an abundance of caution, we want to explain the free services we are making available to help safeguard you against possible identity fraud.

To protect you from potential misuse of your information, **we are offering complimentary credit monitoring services through IDX**, a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. IDX identity protection services include: 24 months 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. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-764-2927 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday, from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 18, 2022.

What You Can Do

We also want to suggest additional steps you might consider taking as well. We have also included details on other precautionary measures you can take to protect your 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.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. 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 at [REDACTED] It is staffed with professionals familiar with this incident and knowledgeable about what you can do to protect against misuse of your information. The response line is available Monday through Friday, from 9 am - 9 pm Eastern Time.

Sincerely,

Newcourse Communications, Inc.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 24-Month Credit Monitoring.

Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial one-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 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 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 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 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 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.

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.

We recommend that you contact your financial institution to inquire about steps to take to protect your loan account.

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.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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.

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/articles/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.

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.

Washington, D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, <https://oag.dc.gov/consumer-protection>, Telephone: 1-202-727-3400.

