McDonald Hopkins
A business advisory and advocacy law firm®

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

P 1.248.646.5070
F 1.248.646.5075

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

September 9, 2021

VIA U.S. MAIL

John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Marine Bank & Trust – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Marine Bank & Trust ("Marine Bank"). I am writing to provide notification of an incident that may affect the security of personal information of two (2) New Hampshire residents. Marine Bank's 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, Marine Bank does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On March 15, 2021, Marine Bank detected potential unauthorized access to its network. Upon learning of this issue, Marine Bank contained and secured the threat and commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals to help determine whether any sensitive data had been compromised because of the incident. Marine Bank's investigation determined that the unauthorized individual(s) potentially removed certain files and folders from portions of its network between February 28, 2021 and March 6, 2021. On August 24, 2021, following an extensive review and analysis of the data at issue, Marine Bank determined that certain files and folders potentially removed from its network may have contained the residents' name, Social Security number, driver's license number, and financial account number.

At the time of this notification, Marine Bank is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Marine Bank 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 residents against identity fraud. Marine Bank is providing the affected residents with written notification of this incident commencing on or about September 8, 2021 in substantially the same form as the letter attached hereto. Marine Bank is offering the affected residents complimentary one-year membership with a credit monitoring service. Marine Bank will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Marine Bank will 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.

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

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,

Colin M. Battersby

Encl.

Marine Bank & Trust

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

[redacted]

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Marine Bank & Trust. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

On March 15, 2021, Marine Bank & Trust detected unauthorized access to its network. Upon learning of this issue, Marine Bank & Trust contained and secured the threat and commenced a prompt and thorough investigation. We launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to help determine whether any sensitive data had been compromised as a result of it. Our investigation determined that the unauthorized individual(s) had access to and potentially removed certain information from portions of our network between February 28, 2021 and March 6, 2021.

On August 24, 2021, following an extensive review and analysis of the data at issue, we determined that the information potentially removed from our network may have included your name, Social Security number, driver's license number, and financial account number.

Given the unauthorized network access, potential acquisition of certain files and the value we place on our relationship with you, we wanted to notify you about this incident.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

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 remain vigilant over the next 12 – 24 months in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

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 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 Monday through Friday, 9am – 9pm Eastern.

Sincerely,

[redacted]

Marine Bank & Trust Company

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website to enroll:** https://www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code:** [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.
You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of 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.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

2. **Placing a Fraud Alert on Your Credit File.**

You may want to consider placing a fraud alert on your credit reports. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified below. Additional information is available at https://www.annualcreditreport.com/index.action.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may contact any one of the three nationwide credit reporting companies below to place a fraud alert on your files. We recommend that you contact one of the credit reporting companies by phone or online to find out the specific requirements and expedite this process. As soon as one credit reporting company confirms your fraud alert, the others are notified to place fraud alerts. After your fraud alert request, all three credit reporting companies will send you one free credit report for your review.

Equifax	*Experian*	*TransUnion*
(800) 525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ P. O. Box 105788 Atlanta, GA 30348	(888) 397-3742 https://www.experian.com/fraud/center.html P. O. Box 9554 Allen, TX 75013	(800) 680-7289 https://www.transunion.com/fraud-alerts P. O. Box 6790 Fullerton, CA 92834-6790

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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

You also have the right to place a security freeze on your credit file. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit file, you need to separately contact each of the three nationwide credit reporting companies. A security freeze can be placed on your credit file at no cost to you. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. We recommend that you contact the credit reporting companies, identified below, by phone or online to find out their specific requirements and expedite this process.

- **Best Practices on Helping to Keep Your Data Secure**
  - Do not share personal information over the phone, through the mail, or over the internet unless you initiated the contact or know the person you are dealing with. If someone contacts you unexpectedly and asks for your personal information, even if it is a company you regularly conduct business with, call the company back directly using the published company phone number to verify the request is legitimate before providing any data;
  - Choose PINs and passwords that would be difficult to guess and avoid using easily identifiable information such as your mother's maiden name, birth dates, the last four digits of your Social Security number, or phone numbers. Also, avoid using the same password for online banking that you use for other accounts. Your online banking password should be unique to that account only;
  - Pay attention to billing cycles and account statements and contact us if you don't receive a monthly bill or statement since identity thieves often divert account documentation;
  - Be careful about where and how you conduct financial transactions, for example, don't use an unsecured Wi-Fi network because someone might be able to access the information you are transmitting or viewing.
  - Monitor your accounts regularly for fraudulent transactions.
  - 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.

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	**Experian Security Freeze**	**TransUnion Security Freeze**
1-800-349-9960 P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	1-888-397-3742 P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze	1-888-909-8872 P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/securityfreeze

4. **Obtaining a Free Credit Report.**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting https://www.annualcreditreport.com/index.action, calling toll-free (877) 322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf, or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies.

Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	*Experian*	*TransUnion*
(800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	(800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Stolen account information is sometimes held for future use or shared among a group of thieves at different times. Checking your credit report periodically can help you spot problems and address them quickly.

5. Review Your Account Statements and Notify Law Enforcement of Suspicious Activity.

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements, from us and others, and monitoring your credit reports closely. If you detect any suspicious activity on any account or have reason to believe your information is being misused, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and the Federal Trade Commission ("FTC"). If you file an identity theft report with your local police department, you should ask for and are entitled to receive a copy of the police report. Some creditors may ask for the information contained in the report.

You may be able to obtain information from your state's attorney general on the steps you can take to avoid identity theft. Contact information for your state's attorney general is available at http://www.naag.org/naag/attorneys-general/whos-my-ag.php.

For information from the FTC on how federal law limits your liability for unauthorized charges to certain accounts, please visit http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

6. 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.

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit https://www.consumer.ftc.gov/topics/identity-theft.

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.

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.

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/,