

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

October 12, 2023

VIA ONLINE SUBMISSION

Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: FNCB Bank – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents FNCB Bank d/b/a 1st Equipment Finance (“FNCB”). I am writing to provide notification of an incident that may affect the security of personal information of approximately one (1) Maine resident. By providing this notice, FNCB does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

On July 12, 2023, FNCB received notice from Darling Financial Group (“DFG”), a third-party vendor, regarding a security vulnerability in the MOVEit Transfer solution that is utilized by DFG. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer, which has been actively exploited by unauthorized actors to gain access to data stored on MOVEit Transfer. There was no compromise of FNCB’s network.

Upon being informed of the vulnerability, DFG immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third party professionals to assist in the investigation and remediation of the vulnerability. Following their investigation, DFG discovered on July 10, 2023, that certain files were removed from its network by an unauthorized party. DFG informed FNCB on July 19, 2023 that the impacted files potentially included FNCB customer information. At that time, FNCB began a comprehensive review of the impacted files and discovered on August 22, 2023 that they contained the personal information of a Maine resident including first and last name, Social Security number and financial account number.

FNCB 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 resident against identity fraud. FNCB is providing the affected resident with written notification of this incident commencing on or about October 12, 2023, in substantially the same form as the letter attached hereto as **Exhibit A**. FNCB is offering the resident a complimentary one-year membership with a credit monitoring service. FNCB will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. FNCB will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At FNCB, protecting the privacy of personal information is a top priority. FNCB is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. FNCB 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.

Exhibit A



100 South Blakely Street
Dunmore, PA 18512
1.877.879.3622 | fncb.com | Member FDIC |

October 12, 2023

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to FNCB Bank d/b/a 1st Equipment Finance (“FNCB”). We are contacting you regarding an incident that impacted Darling Financial Group (“DFG”) (260 Merrimack St. Newburyport, MA 01950), a third-party vendor that offers balance sheet advisory services and expertise, in which some of your personal information was disclosed to an unauthorized party. As such, 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 information.

What Happened

DFG recently advised FNCB that it received notice from one of its third-party vendors regarding a security vulnerability in the MOVEit Transfer solution which is utilized by DFG to transfer FNCB data. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on MOVEit Transfer. MOVEit has acknowledged the vulnerability and provided patches to remediate the exploit. Importantly, the incident did not involve FNCB’s systems nor impact our ability to service our customers.

What We Are Doing.

Upon being informed of the vulnerability, DFG immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third party professionals to assist in the investigation and remediation of the vulnerability. Following their investigation, DFG discovered on July 10, 2023, that certain files that potentially contain personal information were removed from its network by an unauthorized party. DFG informed FNCB on July 19, 2023 that the impacted files potentially included FNCB customer information. At that time, we began a comprehensive review of the impacted files and on August 22, 2023, we discovered that certain personal information was contained within the impacted files that was subject to unauthorized access and acquisition as a result of the incident.

What Information Was Involved?

The information that may have been accessed contained some of your personal information, including your first and last name, Social Security number, and financial account number.

What You Can Do.

We have no evidence that any of your information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and to help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

For more information on identity theft prevention and Experian IdentityWorksSM, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

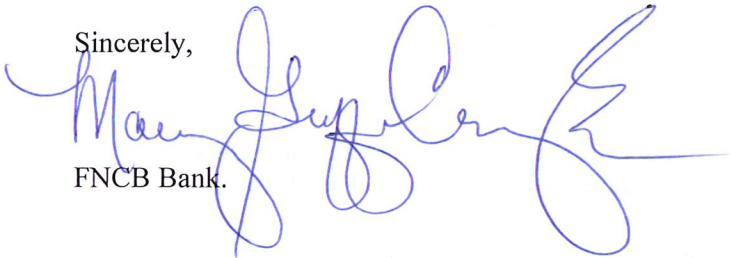
This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

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 toll-free number at 1- [REDACTED] or email us at [REDACTED]. FNCB's Customer Care Center is staffed with professionals familiar with this incident and are knowledgeable on what you can do to protect against misuse of your information. FNCB's Customer Care Center is available Monday through Friday, 8:30 am – 5:00pm EST and Saturday 9:00 am – Noon EST.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Mae J. [REDACTED]', is written over the word 'Sincerely,'. The signature is fluid and cursive.

FNCB Bank.

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Membership Now in Three Easy Steps

1. ENROLL by: **December 11, 2023** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll:
[REDACTED]
3. PROVIDE the **Activation Code:** [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by December 11, 2023. 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 MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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 [REDACTED]
or call [REDACTED] to register with the activation code above.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

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 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.

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.

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, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

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 from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

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.);
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.