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

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

RECEIVED
NOV 14 2022
CONSUMER PROTECTION

November 8, 2022

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Franklin Mint Federal Credit Union ("FMFCU") and State Financial Network ("SFN") – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Franklin Mint Federal Credit Union ("FMFCU") of which State Financial Network ("SFN") is a mortgage subsidiary. I am writing to provide notification of an incident that may affect the security of personal information of two (2) New Hampshire residents. By providing this notice, FMFCU does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

FMFCU recently learned that one of SFN's third-party partners (the "Third Party") experienced a security incident in which an unauthorized individual accessed one (1) employee email account between June 23, 2022 and July 8, 2022. Upon learning of this issue, the Third Party commenced an internal investigation. As part of this investigation, the Third Party has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Based on its comprehensive investigation and manual document review, the Third Party confirmed on September 1, 2022, that the email account contained personal information. SFN and FMFCU were subsequently notified of the incident on October 25, 2022.

At the time of this notification, neither SFN nor FMFCU are aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, FMFCU and SFN 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. FMFCU and SFN are providing the affected resident with written notification of this incident commencing on or about November 4, 2022 in substantially the same form as the letter attached hereto. FMFCU and SFN are providing the affected resident with 12 months of complimentary credit monitoring services and will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. FMFCU and SFN 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

is also being provided with the contact information for the consumer reporting agencies, and the Federal Trade Commission.

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

Should you have any questions regarding this notification, please contact me at (248) 220-1360 or cczuprunski@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Christine N. Czuprynski

StateFinancial
NETWORK

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to State Financial Network ("SFN"), the mortgage servicing subsidiary of Franklin Mint Federal Credit Union. We are writing with important information regarding a recent data security incident that involved some of your information. 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?

We recently learned that one of our Third Party Partners (the "Third Party"), experienced a security incident in which an unauthorized individual accessed one employee email account between June 23, 2022 and July 8, 2022. This unauthorized email access contained some of your personal information.

What Has Been Done

In addition to securing the account, the Third Party commenced an internal investigation as well as engaged a forensic security firm to investigate the incident and confirm the security of the email and computer systems. This investigation determined that an unknown individual accessed the email account for a short period of time from June 23, 2022 to July 8, 2022. The Third Party reviewed the contents of the account to determine if it contained any personal information. On September 1, 2022, the Third Party confirmed that the email account contained personal information. SFN was subsequently notified of the incident on October 25, 2022. While we have no indication or evidence that any of that data has been or will be misused, we thought it important to notify you of this incident.

What Information Was Involved.

Based on the Third Party's investigation and manual document review, we have determined that the compromised email account contained your name, [redacted].

What You Can Do.

We have no evidence that the unauthorized party actually viewed or misused any of your personal information. Nevertheless, out of an abundance of caution, we want to make you aware of the 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.

State Financial Network, LLC
5 Hillman Drive, Suite 300 • Chadds Ford, PA 19317-9998
NMLS # 1020019

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 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 [redacted] at [redacted].

Sincerely,

[redacted]

[redacted]
State Financial Network

StateFinancial
NETWORK

– 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.)
   a. Enrollments must occur by no later than 5:59pm CT.
2. VISIT the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/credit
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 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/credit
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.

* 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.

State Financial Network, LLC
5 Hillman Drive, Suite 300 • Chadds Ford, PA 19317-9998
NMLS # 1020019

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, 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 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	*Experian*	*TransUnion LLC*
P.O. Box 105069	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 2000
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	https://www.experian.com/fraud/center.html	Chester, PA 19016-2000
(800) 525-6285	(888) 397-3742	https://www.transunion.com/fraud-alerts
		(800) 680-7289

3. 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	*Experian Security Freeze*	*TransUnion Security Freeze*
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
https://www.equifax.com/personal/credit-report-services/credit-freeze/	http://experian.com/freeze	https://www.transunion.com/credit-freeze
(888) 298-0045	(888) 397-3742	(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.

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.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.