



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, 36th Fl
Philadelphia, PA 19103
aweaver@constangy.com
Direct: 941.875.5335

July 20, 2023

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Franklin Mint Federal Credit Union ("FMFCU") in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On June 1, 2023, FMFCU became aware of an alert issued the same day by the Cybersecurity and Infrastructure Security Agency ("CISA") addressing a critical vulnerability affecting MOVEit Transfer, a managed file transfer solution used widely by businesses and government agencies, including FMFCU, to securely transfer data. After becoming aware of the alert, FMFCU took immediate steps to patch its MOVEit system in accordance with the software developer's instructions and conduct an internal assessment. FMFCU thereafter undertook a comprehensive investigation with the assistance of leading external experts to learn more about the scope of any potentially affected data.

On June 19, 2023, the investigation revealed that data belonging to FMFCU members may have been acquired without authorization in connection with this issue. FMFCU then worked diligently to identify the potentially affected data elements and gather contact information needed to provide notice to all potentially affected members. This process concluded on June 28, 2023, at which time FMFCU took steps to arrange for individual notification.

2. Number of Maine residents affected.

On July 20, 2023, FMFCU became aware of approximately thirty-seven (37) Maine residents within the potentially affected population. The personal information potentially impacted in connection with this incident includes name, Social Security number, and/or financial account number. FMFCU notified the Maine residents of this incident via First Class U.S. mail beginning on June 20, 2023, via the attached sample notification letter or a substantially similar version thereof. In so doing, FMFCU provided individuals with steps they can take to protect their personal information and offered them twelve months of free credit and identity monitoring services through Experian.

July 20, 2023

Page 2

3. Steps taken relating to the Incident.

As soon as FMFCU discovered this incident, FMFCU took steps to quarantine the affected MOVEit system and implemented remediation measures recommended by the MOVEit software developers. Further, FMFCU reported this matter to law enforcement and will cooperate in any resulting investigation.

FMFCU has also established a toll-free call center through Kroll to answer questions about the incident and related concerns, and provided additional member resources through its website.

4. Contact information.

FMFCU remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

A handwritten signature in black ink, appearing to read 'Aubrey Weaver', with a stylized, flowing script.

Aubrey Weaver
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Subject: [Notice of Data Incident] [Notice of Data Breach])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Franklin Mint Federal Credit Union (“FMFCU”) is writing to inform you of a recent data security incident that may have affected your personal information. FMFCU is one of an estimated 2,500 organizations worldwide recently affected by the MOVEit software vulnerability. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened? On June 1, 2023, FMFCU became aware of an alert issued the same day by the Cybersecurity and Infrastructure Security Agency (“CISA”) addressing a critical vulnerability affecting MOVEit Transfer, a managed file transfer solution used widely by businesses and government agencies, including FMFCU, to securely transfer data. After becoming aware of the alert, FMFCU took immediate steps to patch its MOVEit system in accordance with the developer’s instructions and conduct an internal assessment. FMFCU thereafter undertook a comprehensive investigation with the assistance of leading external experts to learn more about the scope of any potentially affected data. On June 19, 2023, the investigation revealed that data belonging to FMFCU members may have been acquired without authorization in connection with this issue. Since that time, FMFCU has been collecting information needed to provide notice to all potentially affected members.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your <<b2b_text_2(data elements)>>. The potentially affected information may have also included your member number.<<b2b_text_3(“Insert1” The potentially affected information also included your partial credit card number.)>><<b2b_text_4(“Insert2” Due to FMFCU’s partnership with an external loan provider, the potentially affected information may have also included information related to a personal loan purchased by FMFCU.>>

What Are We Doing? As soon as FMFCU discovered this incident, the above described steps were taken. In addition, FMFCU reported the incident to law enforcement and will cooperate with any requests for information related to this issue. We have quarantined the affected MOVEit system and taken all remediation measures recommended by the MOVEit software developers. FMFCU will also be evaluating additional safeguards that can be put in place to further enhance the security of the data entrusted to us.

FMFCU also leverages advanced monitoring tools to help identify any suspicious transactions on member accounts. As an additional resource to help protect your information, FMFCU is offering individuals whose information was involved in this incident complimentary access to Experian IdentityWorksSM for 12 months. If you believe there has been unauthorized use of your information and want to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping with contacting credit grantors to dispute charges and close accounts; assisting in placing a freeze on your credit file with the three major credit bureaus; and assisting with contacting government agencies to help restore your identity to its proper condition).

Please note Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, FMFCU also encourages you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12 month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, follow the steps below:

- Ensure you enroll by <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code:<<activation code s_n>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or want an alternative to enrolling in Experian IdentityWorks online, contact Experian's customer care team at 1-877-288-8057 by <<b2b_text_6(activation deadline)>>. Be prepared to provide engagement number <<b2b_text_5(engagement number)>> 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:

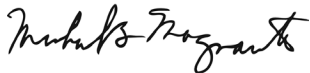
- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- Identity Restoration: Identity Restoration 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 Insurance²: Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. We also encourage you to take advantage of the complimentary identity protection services being offered through Experian. Visit FMFCU's web page for this incident at www.fmfcu.org/securityincident for additional information on how to protect your accounts and how to opt-in to purchase and security alerts.

For More Information: Further information on protecting your personal information appears on the following page. If you have questions about this issue, please call the dedicated call center for this incident at (866) 373-9037 from 9:00 AM to 6:30 PM Eastern Time, Monday through Friday (excluding major U.S. holidays). Call center representatives are fully versed on this incident and can answer your questions.

Rest assured, FMFCU takes the privacy and security of member information very seriously. Our sincerest apologies for any worry or inconvenience this may have caused you.

Sincerely,



Michael B Magnavita, CPA
President and CEO

Franklin Mint Federal Credit Union
5 Hillman Drive, Suite 100
Chadds Ford, PA 19317

¹Offline members are eligible to call for additional reports quarterly after enrolling.

²The 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.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and stays on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests 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 above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This prevents new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903 <http://www.riag.ri.gov>
www.riag.ri.gov
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf