



30219

Exhibit A

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

[Date]

RE: Important Security Notification. Please read this entire letter.

Dear [First Name] [Last Name]:

American First Credit Union ("American First") recently discovered an incident involving a security event impacting a software application that is used by one of our vendors, Darling Consulting Group, Inc. ("DCG"), which may affect the security of your personal information. Please note that American First, itself, has not suffered a security event on its systems, and your personal information in American First's custody was not impacted by the incident. Although we have no indication of identity theft or fraud in relation to this event, we want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? American First has a vendor relationship with DCG, which stores and/or transfers personal information using the MOVEit Transfer software called Progress Software to provide services to American First. American First utilizes MOVEit in the regular course of business operations to securely transfer files. On or around July 24, 2023, DCG disclosed a vulnerability in the MOVEit Transfer software that had been exploited by an unauthorized third party on or around May 31, 2023, that involved your information. American First Credit Union promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on your account. Through the investigation, we learned that a third party accessed our files within the MOVEit application and downloaded a file containing some of your personal information. When we became aware of this incident, we connected with DCG, and we were advised by DCG that it had already commenced action to mitigate the security event. DCG retained cybersecurity experts and advisers to assist in evaluating the situation and notified applicable law enforcement, among other mitigation steps. American First also activated its own incident response procedures to ensure that the security event did not impact its systems.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the file that was accessed: Full Account Name, Loan Account Number and Loan Principal Balance. At this time, we are not aware of any actual or attempted misuse of your personal information.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Safeguarding our members' information is a top priority. Upon learning about this vulnerability, investigate the root cause of the issue, asses the security of the MOVEit application and notify potentially affected members. We are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this incident, as an additional precaution, American First credit Union is offering you access to 12 months of complimentary credit monitoring and identity restoration services through Experian. Details of this offer and instructions on how to activate these services are listed below.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12-months.

If you believe there was fraudulent use of your information as a result of this incident and would like 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 that 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 you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 3 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage 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, please follow the steps below:

- Ensure that you **enroll by 10/31/2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [https:// www.experianidworks.com/3bcredit](https://www.experianidworks.com/3bcredit)
- Provide your **activation code**: [Activation Code]

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 1-877-890-9332 by **10/31/2023**. Be prepared to provide engagement number **B100340** as proof of eligibility for the Identity Restoration services by Experian.

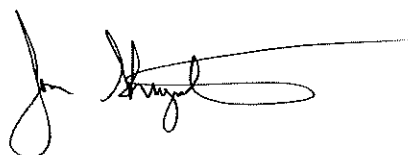
ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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, 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 Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 800-290-1112.

Sincerely,



Jon Shigematsu,
CEO/President

* 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.

Attachment A – Information for U.S. Residents

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other 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. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
<http://www.identitytheft.gov/>
1-877-IDTHEFT (438-4338)

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 <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:
equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Experian:
experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:
transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at <http://www.dos.ny.gov/consumerprotection> or (800) 697-1220 or NYS Attorney General at <http://www.ag.ny.gov/home.html> or (800) 771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For New York and North Carolina residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).