BUTLER | SNOW

May 4, 2015

Via FedEx Overnight Courier

Office of the Attorney General
ATTN: Consumer Protection Division
33 Capitol Street
Concord, NH 03301

Ladies and Gentlemen:

Pursuant to NH Rev. Stat. Ann. 359-C:20, we are writing on behalf of our client, Fort Campbell Federal Credit Union with its principal office in Clarksville, Tennessee (the "Credit Union" or "Client"), to notify your office of an inadvertent disclosure of personal information involving one New Hampshire resident, who is a member of the Credit Union.

On or around April 7, 2015, Credit Union management became aware that a third-party vendor contracted to produce and mail member statements and various other account notices to Credit Union members inadvertently mailed overdraft notices to a number of our members, including notices intended for other Credit Union members. The overdraft notices included the names, mailing addresses, member numbers and account balances. While our Client does not have any indication that the information has been used improperly, the Credit Union is taking prompt, appropriate precautionary actions to notify affected members and to prevent and detect any attempted misuse of member information.

Upon discovery of the incident described above, the Credit Union took immediate steps to investigate the incident. During the course of the investigation to date, the Credit Union determined that, according to the third party vendor, a printing error occurred after a Credit Union staff member requested a signature block modification to reflect a recent personnel change. Apparently, the modification effected by our Client's vendor caused some end-of-file/end-of-page markers to be altered so that a number of unrelated (by member number) notices were grouped together under one individual member number instead of being processed separately. The modification also caused full disclosure of the member number which is normally truncated.

Additional research indicates the erroneous mailings occurred during the period March 12 to April 6, 2015 and involved 1,523 notices mailed to 36 individual members. Taking into account that multiple notices were generated for some accounts, it has been determined there were 1,307 members involved (out of a total membership of 48,943) including the 36 intended recipients. In some cases (357 of the 1,307) electronic notices were generated for access via our home banking

web site; the remaining (951 of 1,307) were mailed. The Credit Union's IT staff was able to identify those members (of the 36) who actually viewed the notices online; if IT determined the notices were not viewed, they were removed from the online application (review indicates most members had not viewed/accessed the notices).

In response to the incident our Client has, to date, taken the following steps to eliminate or mitigate any potential consequences to the members involved:

- The Credit Union contacted its third party vendor to ensure no further occurrences immediately after learning of the error.
- Our Client's bonding company has been placed on notice.
- The Credit Union attempted to contact each member who received erroneous notices and requested they return them to the Credit Union if still in their possession. Staff also contacted local area post offices and were able to intercept a portion of the notices mailed just prior to the Credit Union learning of the error.
- Warnings were placed on all affected member accounts so that when an individual contacts the Credit Union to conduct a transaction, whether in person or by telephone, they will be asked to provide supplemental identifying information.
- All affected members will soon receive written notice of the incident and an offer for one year of complimentary credit monitoring. A copy of the form notice is enclosed.

The information erroneously divulged (i.e., the member number) cannot be used to access an account via remote/electronic means. Our Client's system requires the use of additional information to effect any type of electronic transaction.

Our Client takes this matter seriously and has taken, and continues to take, appropriate actions to eliminate or reduce the consequences of this event.

Please do not hesitate to contact the undersigned at either [redacted] or [redacted] should you have any questions or require further information. Thank you.

Very truly yours,

[redacted]

Enclosure as stated

c[redacted]

[Company Logo]

[Return Address]
[Date]

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

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

Dear [Insert customer name]:

We are contacting you regarding a data security incident that occurred during the period March 12 – April 6, 2015. This incident involved disclosure of your name, address, Fort Campbell Federal Credit Union member number, and account balance. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

An investigation of this incident revealed that the source of the disclosure was a Credit Union vendor. The third-party vendor, contracted to produce and mail statements and various other account information, inadvertently mailed overdraft notices to a number of Credit Union members, including notices intended for other members. However, no Personal Identification Numbers (PINs) were disclosed.

There is no indication that your information has been used improperly, but we are notifying affected members and taking action to minimize or eliminate potential harm. We strongly encourage you to take precautionary measures now to help prevent and detect any attempted misuse of your information. We also recommend reviewing the online guidance provided by the Federal Trade Commission ("FTC") regarding steps you can take to protect against identity theft. Contact information is provided below.

What we are doing to protect your information:
To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: August 8, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide Engagement #: **[Engagement number].**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, 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 877-371-7902.

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 the final page of this letter.

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the product and options outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at [insert company phone number].

Sincerely,
[Signed by appropriate executive]

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

Please be sure to inquire about any fees that may be assessed by the credit reporting companies for placing, lifting or removing a security freeze. In some cases, you may be charged up to $10.00 per transaction.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228. 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.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

➢ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF:** Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you are encouraged to contact the Federal Trade Commission. You can obtain information from the FTC about steps an individual can take to avoid identity theft.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338
TTY: 1-866-653-4261