NAVY FEDERAL Credit Union

October 6, 2017

<Member Name>
<Address 1>
<Address 2>
<City>, <State> <Zip Code>

Dear <Member Name>:

We are writing to notify you of an incident involving unauthorized access to your personal and financial information. This incident was not part of a cyber attack on Navy Federal systems, but rather it was related to an individual's criminal activity. We are working with law enforcement authorities to assist them in their investigation. Promptly after learning of the incident, we conducted a thorough review of your accounts for possible fraudulent activity and placed them under close supervision for continued monitoring. Our team continues to monitor your accounts closely, and we ask that you contact one of our specialists in our Security Operations Center at the number below should you have any concerns.

Please understand information security is a top priority of Navy Federal, and we are committed to protecting your accounts from fraud. We will soon be contacting you by phone to discuss additional steps you may wish to take to protect your information. In the interim, if you have any questions regarding this incident, please call our **Security Operations Center at 1-866-661-7655**.

As an added protective measure, we would like to provide you with free identity protection and credit monitoring services for two years. The enclosed official notice provides additional details, including how to activate your free identity protection and credit monitoring services.

We regret any inconvenience this may cause you. We value and thank you for your membership at Navy Federal Credit Union.

Sincerely,

Robert A. Carlisle

Robert A. Carlisle
Chief Security Officer

NAVY FEDERAL Credit Union

Official Notice

Navy Federal Credit Union learned in September of an incident involving the unauthorized reproduction of your personal and financial information at Navy Federal. Promptly after learning of the incident, we conducted a thorough review of your accounts for possible fraudulent activity and placed them under close supervision for continued monitoring. Our team continues to monitor your accounts closely. We are working with law enforcement authorities to assist them in their investigation. This incident occurred between December 2014 and December 2016 and included the following types of information: first and last name, Social Security number, date of birth, address, e-mail address, account number, code word, and phone number.

We will soon be contacting you by phone to discuss steps you may wish to take to protect your information. In the interim, if you have any questions regarding this incident, please call our **Security Operations Center at 1-866-661-7655**.

Account Reset. Please understand that we consider the safeguarding of our members' personal information a top priority. The affected accounts at Navy Federal Credit Union are now under close supervision for unusual activity, and we are committed to protecting those accounts from fraud arising from this incident. We will assist you with resetting your Navy Federal information, including account numbers, passwords, telephone PIN, and code words, as appropriate.

Free Identity Protection And Credit Monitoring Services. To help you protect your identity and your credit information, we have arranged with AllClear ID to offer you free identity protection and credit monitoring services for 24 months. The following services start on the date of this notice and you can use them at any time during the next 24 months:

> AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
>
> AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide certain information.

You may sign up online at enroll.allclearid.com using the following redemption code: <Unique Redemption Code>.

Order Your Free Credit Report. In addition, you can take other steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request

PO Box 3000 Merrifield VA 22119-3000

Service, PO Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

We encourage you to act now and remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the credit union. We recommend that you review your account statements and obtain your free credit reports. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors and unauthorized activity in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to law enforcement authorities because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your financial institution or payment card company. If you detect the establishment of an unauthorized account or any other incident of identity theft or fraud, promptly report the incident to local law enforcement authorities, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of

identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. PO Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. PO Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC PO Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, contact the three nationwide consumer reporting agencies or the FTC as described above.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400