November 30, 2011

JEANNE D'ARC
CREDIT UNION

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301-6397

Dear Attorney General Delaney:

I am providing this letter as notice pursuant to New Hampshire Revised Statutes Annotated Chapter 359-C, Section 20 of an unauthorized disclosure of personal information involving approximately 327 New Hampshire members or former members of Jeanne D'Arc Credit Union, a Massachusetts state chartered credit union. There has not been any unauthorized use of the disclosed personal information, but the acquisition of the personal information in question was in violation of Jeanne D'Arc Credit Union policies and was not authorized. For the reasons outlined below, we do not believe that the unauthorized disclosure creates a risk of identity theft or fraud against any of the affected members of Jeanne D'Arc Credit Union, but we nevertheless have determined that the more prudent course of action is to provide this notice.

The incident giving rise to this notice occurred when a departing employee voluntarily left Jeanne D'Arc Credit Union to take a position at another financial institution. The employee left employment with Jeanne D'Arc on December 27, 2010, and used a USB thumb drive device to copy and take a number of forms and documents that she planned to make use of in her new position. We only learned of this disclosure on July 29, 2011, after our former employee left her new position. Upon her departure from her new position, her employer reviewed the employee's computer, discovered computer files that originated at Jeanne D'Arc, and sent us a disk containing copies of the files. We then engaged FIS Governmental Services, a division of Fidelity National Informational Services, Inc. to perform an analysis of the disclosed computer files. FIS has substantial experience in advising clients about data security breaches and has expertise and capability to conduct computer forensic analysis. The report FIS prepared for us contains personal information of our members, but we would be happy to provide a copy of the FIS report should you so require.

The FIS report indicates, and we have confirmed, that the personal information disclosed was primarily contained in 2 groups of computer files. One group contained real estate tax escrow analysis reports that include each member's name and social security number. The second group contained loan servicing reports that contain each member's name and mortgage loan account number. Because the social security number and the name combined with an account number constitute personal information, we will be providing notice to each of our members whose information was included in the disclosed computer files. A copy of the notice is

We have also taken the following steps in addition to obtaining the FIS report described above. We have recovered the thumb drive device that contained the computer files in question. We have obtained a sworn affidavit from our former employee indicating that she made no unauthorized use or further disclosure of the disclosed personal information. Our former employee has made available for our inspection, and we have inspected and determined, that the former employee did not copy the personal information to her own personal computer. We have also received assurances from our former employee's subsequent employer that it has taken appropriate safeguards to prevent further disclosure of the personal information. That party is a financial institution and we understand that it will take the same measures to protect the disclosed information as it takes to protect its own customers' personal information. For the foregoing reasons, we think that the disclosed personal information has been recovered and adequately protected and do not believe that the unauthorized disclosure creates a substantial risk of identity theft or fraud against any of our affected members.

We have also implemented new measures to help prevent a future occurrence of a similar incident. It is important to note that the employee who caused the unauthorized disclosure was an officer who had access to computer files that the typical employee does not have. Nevertheless, we are in the process of implementing more secure monitoring software that will alert our IT department when a large amount of files are being copied to any removable media. For those employees who have a need to copy files to removable media, they will only have the ability to copy those files to encrypted, password protected media. These measures will be fully implemented no later than the end of December, 2011, and we are confident these measures will greatly reduce the likelihood of a further occurrence. We have also taken this opportunity to re-notify all of our employees of our data security and ethics policies, and to illustrate to them the severe consequences that can result from even an unintentional breach of security.

We will be providing a copy of this letter to the Commissioner of Banks. Please let me know if you have questions regarding any of the foregoing or if you require further information.

Sincerely,

Mark S. Cochran

Enclosure
MSC: pc

cc: New Hampshire Commissioner of Banks
53 Regional Drive, Suite 200
Concord, NH 03301

JEANNE D'ARC
CREDIT UNION

SAMPLE LETTER TO AFFECTED JEANNE D'ARC CREDIT UNION MEMBERS

Date

Consumer Name
Address
City, ST

Dear _

This letter is being provided to you under the provisions of various state laws that require notice to consumers of breaches of data security protocols. We are required to notify you when certain personal information is disclosed or acquired by an unauthorized party. Personal information is defined by law to include your social security number, or your bank account number when included in a record with your first name or initial and your last name. This letter is to inform you that an unauthorized disclosure of your personal information occurred within the last year, on or about December 27, 2010. We discovered the disclosure many months after it occurred, and do not believe there has been any unauthorized use made of your personal information.

We are required to provide you with notice of certain rights you have when such an incident occurs, including the right to place a security freeze on your credit reports and the rights to obtain and file police reports. These rights are summarized in the enclosed NOTICE OF IMPORTANT RIGHTS form, and we urge you to read and carefully review the entire enclosed form.

We regret that this incident occurred. We suggest that all of our members regularly review credit card and other financial accounts statements for any suspicious and/or unauthorized activity, and also periodically review credit reports for unexplained activity. In addition the credit freeze procedures described in the enclosed notice, there are a number of companies that offer credit monitoring services for a monthly or annual fee to those who choose to subscribe to such services. Should you have further questions about this matter, please feel free to contact Jeanne D'Arc Credit Union at 978-452-5001.

Sincerely,

Scott Flagg
Senior Vice President
Chief Member Service Officer

NOTICE OF IMPORTANT RIGHTS

You have the right to obtain any police report filed in regard to 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. You also have the right to place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift. or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Your social security number;
3. Your date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of your current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card such as a state driver's license or ID card or military identification;
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.