



March 15, 2013

##90561-LV1-0123456 T-0012 \*\*\*\*\*5-DIGIT 12345

SAMPLE A SAMPLE

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



I am writing to make you aware that United Shore Financial Services, LLC ("USFS") recently discovered that it was the victim of a computer intrusion by an unauthorized third party. The server that was accessed may have contained your personal information, including your name, contact information, date of birth, driver's license number, social security number and financial account information you may have previously provided to us. We believe the incident began on December 2, 2012. USFS became aware of the incident on January 31, 2013, and immediately hired outside consultants to conduct an exhaustive investigation of the matter, promptly notified the Federal Bureau of Investigation, coordinated our investigative efforts with the U.S. Secret Service Electronic Crimes Task Force, and took several steps to stop these individuals from continuing to access our systems and your information. These steps included changing account passwords, disabling accounts, updating application code, and adding additional monitoring procedures to our databases and systems.

Although our investigation has not suggested that your information has been misused, we take this matter very seriously and want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, the Attorney General, or the Federal Trade Commission (the "FTC").

To further assist you, we have arranged for you to receive 12 months of free identity protection through Experian's ProtectMyID™ Alert program. This membership includes identity theft resolution services, a free credit report, daily credit monitoring to detect suspicious activity, and a \$1 million\* identity theft insurance policy, including coverage of unauthorized electronic fund transfers from your bank account. To offer added protection, you will receive ExtendCARE™, which will provide you with fraud resolution support even after your ProtectMyID membership has expired. Again, this protection is being offered at no cost to you.

You can register for these services by visiting the ProtectMyID Web Site: [www.protectmyid.com/alert](http://www.protectmyid.com/alert) or calling (877) 297-7780 and providing the following activation code: ABCDEFGHIJKL. You have until June 30, 2013 to register. Enrollment in ProtectMyID membership does not affect your credit score.

You can also place a fraud alert with the major credit reporting agencies on your credit files, their contact information is as follows:

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	Experian Fraud Reporting P.O. Box 9554 Allen, Texas 75013	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	TransUnion LLC P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

\* Identity theft insurance is underwritten by insurance company subsidiaries of Chartis, Inc. The description provided in this letter 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.





A fraud alert lasts 90 days, and requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name (as soon as one agency is notified, the others are notified to place fraud alerts as well). When you contact these agencies, you can also request that they provide a copy of your credit report. Review your reports carefully to ensure that the information contained in them is accurate. If you see anything on your credit reports or credit card account statements that appear incorrect, contact the credit reporting agency or your credit card provider, and report suspected incidents of identity theft to local law enforcement, the Attorney General, or the FTC. Even if you do not find any signs of fraud on your reports or account statements, the FTC and other security experts suggest that you check your credit reports and account statements periodically. You can keep the fraud alert in place at the credit reporting agencies by calling again after 90 days.

You can also ask these same credit reporting agencies to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. 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 want to have a security freeze placed on your account, the reporting agencies will ask you for certain information about yourself. This will vary depending on where you live and the credit reporting agency, but normally includes your name, social security number, date of birth, and current and prior addresses (and proof thereof), and a copy of government-issued identification. The cost to place, temporarily lift, or permanently lift a credit freeze varies by state, but generally, the credit reporting agencies will charge \$5.00, unless you have a police report, in which case it may be free. You have the right to a police report under certain state laws.

If you detect any unauthorized charges on your credit or debit card(s), we strongly suggest that you contact your card issuer by calling the toll-free number located on the back of your card or on your monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. You should tell your card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your card web account password immediately when you discover unauthorized charges.

Finally, the FTC, the Attorney General and the major credit reporting agencies listed above can provide additional information on how to avoid identity theft, how to place a fraud alert, and how to place a security freeze on your credit report. You can contact the FTC on its toll-free Identity Theft helpline: 1-877-438-4338. The FTC's website is located at <http://www.ftc.gov/idtheft> and its address is Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

In Maryland, you can reach the State Attorney General's office by phone at (888) 743-0023. Its website is <http://www.oag.state.md.us/>. In North Carolina, you can reach the State Attorney General's office by phone at (919) 716-6400. Its website is <http://www.ncdoj.gov>. Their mailing addresses are:

Douglas F. Gansler  
Attorney General of the State of Maryland  
Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202

Roy A. Cooper  
Attorney General of the State of North Carolina  
Consumer Protection Division, Attorney General's  
Mail Service Center 9001  
Raleigh, NC 27699-9001

We regret any inconvenience this matter may cause you. I can assure you that we are doing everything we can to protect our customers and ensure nothing like this happens again. If you have questions about this notice or this incident or require further assistance, you can reach us toll free at (855) 770-0003, Monday through Friday between 9:00 a.m. and 6:00 p.m. EST. When prompted, please enter the following 10-digit reference number: 7467031413.

Thank you,

Erin Castro  
Vice President  
Shore Mortgage, a division of USFS

