



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

November 9, 2017

Dear John Sample:

I am writing to you with important information about a recent exposure of your personal information by the State of Maine's Office of Information Technology (OIT). While we do not know of any current misuse or any intent to misuse your information, we are providing this notice out of an abundance of caution and informing you about steps you may take to protect your personal information going forward.

On September 21, 2017, as part of a technology system upgrade, a contractor with OIT posted information from a Maine Department of Health and Human Services (DHHS) child welfare services database to a third-party website outside the State of Maine system. The information was available for approximately four and a half hours before being taken down.

Upon investigation, OIT received assurances from the third-party website that the information was removed from their web server and that no copy of the information remains in their custody. However, OIT has also been informed that the posted information was accessed once during the time it was publicly available.

Unfortunately, it was determined that your information was contained in the exposed file. The personal information in the file included names, addresses, and Social Security numbers of persons receiving foster care benefits, as well as the names of children and legal guardians.

This incident is of great concern to both the Office of Information Technology and the Department of Health and Human Services. Both agencies are working diligently to provide information to all affected clients. We value our relationship with our customers, the people of Maine, and take their trust in us seriously. We apologize for the inconvenience this may cause and assure you that steps are being taken to ensure such an exposure does not occur again.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-609-5573 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 your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-609-5573 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We also advise you to take the following steps immediately:

Call the toll-free numbers of one of the three major credit bureaus listed below to place a 90-day fraud alert on your credit reports. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report. You may extend the 90-day alert by calling for an extension after the initial 90 days.

- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241 [*Please be advised of the recent "Equifax Cybersecurity Incident," see <http://www.equifaxsecurity2017.com>*]

Review and continue to monitor your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report, and under Maine law, you are also entitled to a free credit report from the three reporting agencies each year by visiting <https://www.annualcreditreport.com>. When you receive your credit reports, examine them closely and look for signs of fraud, such as credit accounts that are not yours. Even if you have placed a fraud alert on your account, you should continue to monitor your credit reports to ensure that your personal information has not been misused.

You can also file for a credit report freeze at each of these links to the three Credit Reporting Agencies:

- Experian, <https://www.experian.com/freeze/center.html>
- TransUnion, <http://www.transunion.com/securityfreeze>
- Equifax, <https://www.freeze.equifax.com>

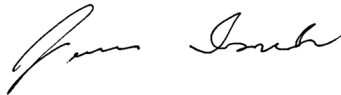
Maine law allows you to freeze your credit report free of charge. A credit freeze will prevent unauthorized parties from accessing your credit report unless you give them specific permission. Freezing your credit will not affect your credit score. For more information on implementing a credit report file freeze, go to the Bureau of Consumer Credit Protection's website, http://www.maine.gov/pfr/consumercredit/file_freeze_info.htm.

Detailed instructions for taking these steps are available on the Department of Professional and Financial Regulation's website, http://www.maine.gov/pfr/financialinstitutions/consumer/credit_report.htm.

If you have any questions with regard to potential identity theft, the Attorney General's Office Consumer Line is 1-800-436-2131, which is open Monday through Friday, 9 a.m. to noon and 1 p.m. to 4 p.m.

Although there is no indication that there is any intent by a third party to misuse your personal data, we are advising all affected individuals of the exposure of their data so that you may take advantage of these precautionary measures at no cost to you. We take seriously our role of safeguarding your personal information and using it in an appropriate manner.

Sincerely,



Jim Smith
Chief Information Officer

