Louisiana Office of Student Financial Assistance

Q: What happened? How did this breach occur?

A: On September 20, 2007, Iron Mountain Incorporated, the state's contractor for data storage, informed the Louisiana Office of Student Financial Assistance (LOSFA) that it had lost some of this agency's backup media on the morning of September 19, 2007. The lost media includes some personal data on residents of the State of Louisiana, many of whom are past or present students at our postsecondary institutions. This sensitive data includes loan extract data for all loans guaranteed by this agency, START Saving Program data on account owners and beneficiaries, and scholarship and state grant data that includes FAFSA and ACT records.

It is important to know that off-site storage is often used as a method to prevent total data loss in the event of a natural disaster, fire, or other event which could completely destroy the facility. The backup media was transferred from the contractor's storage facility to a contractor delivery vehicle for return to the LOSFA facility. It is the responsibility of the contractor to store, transport, and safeguard the backup set in another location. At some time between receipt of the media by the contractor's delivery truck, and delivery of the media to the LOFSA facility, the backup disappeared. Unfortunately, the loss of this backup data does put personal information at risk.

The backup data is compressed and requires special software, specific computer equipment and sophisticated computer skills to access it. We have no reason to believe that the information has been accessed, that it has been misused in any way, or that it will be misused. This loss has been reported and is currently being investigated by the Louisiana Attorney General's office and the Louisiana State Police. There is no indication, so far, of any use of the backup data for malicious intent.

In the interest of consumer protection, LOSFA has set up this web site to assist those potentially affected by this incident in taking measures to ensure that their personal information has not been used for malicious purposes.

Q: Why did LOSFA wait to notify individuals affected?

A: LOSFA took the time to confirm that the data were actually lost rather than misplaced by the contractor. Simultaneously the agency took steps, in accordance with state statute, to ensure that the proper authorities were notified so that a thorough investigation could commence and that the appropriate state agencies and resource entities were brought in to collaborate on action steps before and after notification.

Q: What methods did LOSFA use to notify the public?

A: State statute allows us to make public notice using the media particularly in cases such as this that involve a substantial number of records. Information regarding the data security breach was announced publicly via press release on October 15. Information regarding the breach was simultaneously posted on LOSFA's website. In addition the agency established call centers to handle initial inquiries related to precautionary steps and secondary inquiries related to steps to take if irregularities are subsequently noticed on credit reports received. In addition individual notifications were sent to populations with banking information in the files for ACH transfers which included START savings account holders and some defaulted borrowers in repayment.

Q: What Groups Were Potentially Affected?

A: The lost media includes some personal information on individuals participating in, or considered for participation in, programs administered by LOSFA.

- Anyone who has a Louisiana College Savings account (START Saving Program).
- Any resident of the state of Louisiana who has completed a Free Application for Federal Student Aid (FAFSA).
- Anyone has who completed a FAFSA and included a Louisiana postsecondary institution as an institution to which FAFSA data should be sent.
- Anyone who has applied for or received a Tuition Opportunity Program for Students (TOPS) Scholarship.
- Anyone who has applied for or who has received student financial aid in the State of Louisiana.

Q: What personal information was exposed?

A: The vast majority of these records contained names, date of birth, and Social Security Numbers, and no financial data. However, this data did include financial records for a small percentage of the potentially exposed records,

The only banking information exposed was that provided to LOSFA to enable ACH automatic payments from the individual's bank account to the START Savings account or to repay a defaulted student loan. This account information was needed to enable ACH automatic payments from the individual's bank account to the START Savings account or financial assistance loan account.

Q. What personal information was NOT exposed?

A: Credit card numbers and financial account numbers, with the exception of those that involved bank account numbers that were provided to LOSFA to enable ACH automatic payments from the individual's bank account to the START Savings account or to repay a defaulted student loan. This account information was needed to enable ACH automatic payments from the individual's bank account to the START Savings account or financial assistance loan account

Q: Is this being investigated?

A: Yes, the agency continues to work with various agencies, including the Attorney General's office, to fully investigate this matter and take any action that may be appropriate.

Q: Has anyone been arrested?

A: No. At this time, we understand that the investigation is still on-going.

Q: Do I need to close all of my bank accounts?

A: If you receive a breach notification letter from LOSFA, indicating financial records were exposed (a START savings account or a defaulted student loan) with LOSFA during those years involved), then just those affected accounts must be closed.

- Close the account and open a new one
- Request that the old account be flagged as "closed due to security breach"
- Request that the bank send a letter to the account holder verifying that the account has been closed and flagged.
- Password Protect New Account - a password should not be a mother's maiden name. If the bank insists on a mother's maiden name then make one up. A strong password should be more than 8 characters in length, and contain both capital letters and at least one numeric or other non alphabetical character. Use of non-dictionary words is also advised.

Q: Do I need to close bank accounts, if I did not receive a breach letter?

A: If you do not receive a breach letter from LOSFA, or did not have a Louisiana College savings account (START Saving Program) with LOSFA during the years involved, then NO, you do not need to close your bank accounts. This type of data was not exposed in your particular circumstance.

Q: Do I need to close all of my credit cards?

A: No, you do not need to close credit card accounts because of the potential data exposure. This type of data was not exposed in your circumstance.

Q: What should I do to protect my information?

A: LOSFA has no reason to believe that any of the data in question was accessed with malicious intent. However, as a precautionary step, we suggest that those whose information has been potentially exposed should contact the three credit reporting agencies to place a free 90-day fraud alert on their credit reports.

Experian (888) 397-3742

Equifax (800) 525-6285

TransUnion (800) 680-7289

Please note: Enrolling for a fraud alert will require you to submit personal information, such as your social security number and other personal data. Be aware this is an automated phone system and you will be responding to computer prompts.

In addition, it is strongly recommended that you call all three directly rather than depending upon one agency to contact the other two. Also, these fraud alerts should be renewed every 90 days for at least a year.

Contacting the credit reporting agencies, outside of the fraud alert phone number system, will most likely result in you receiving a credit monitoring product service offering. This is a fee-based service.

Q: I contacted the numbers for the credit reporting agencies and the system said my information did not match what was on file. What do I do now? What does that mean?

A: The computer system will provide you with a list of documents that you must copy and send to a specific post office box for the specific credit reporting agency. We suggest that if you are required to submit this material that you send it U.S.P.S., certified mail return receipt requested.

What this indicates is that the computer cannot verify your identity based upon the responses you have entered. Few people will encounter this problem.

Q: Why can’t I talk to someone “live" to put a fraud alert on my credit report?

A: All three major credit reporting agencies use an automated phone system for setting up the fraud alert and are not generally able to place fraud alert requests "live."

Q: Should I be concerned about giving them my Social Security number.

A: No**.** Credit agencies will need to verify your identity which will require use of your SSN and other similar information. The credit reporting agencies already have this information on file and must use this piece of information to authenticate you.

Q: What is a fraud alert? How will that affect me?

A: A fraud alert is a consumer statement on your credit report which states: "Do not open lines of credit without contacting me first!" It is active for 90 days and should be renewed every 90 days for at least a year.

A fraud alert does not affect your credit score. Also, a fraud alert has no effect on your existing credit accounts or credit cards. It is a warning to credit grantors to contact you first to confirm that you did make a request for credit.

Q: Are there drawbacks to placing a fraud alert?

A: You will be unable to obtain instant credit. You must be available by phone to approve opening a new credit account. If you are not available, the creditor may not open the account. It may take longer to obtain credit and some creditors may be hesitant to open a new account.

A. Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is required by law to make an attempt to contact you if you have a fraud alert in place. A fraud alert does not stop a creditor from granting credit.

Q: What happens when I place a fraud alert?

A: You should receive a notification letter from each of the credit reporting agencies confirming that a fraud alert is in place. Included in these letters will be the steps for obtaining a free copy of your consumer credit reports. It is strongly recommended that you request these reports. The CRAs will only provide you with one copy of the free credit report annually from placing a fraud alert.

In most cases, if identity theft has occurred, it will appear on your credit reports. It will take approximately 7-14 business days to receive your credit reports.

Q: Why can't the LOSFA do the fraud alert with the credit agencies for me?

A: Under federal law, the Fair Credit Reporting Act, each individual must initiate the action. This is a protection for all individuals to prevent malicious applications of fraud alerts. LOSFA is not authorized to initiate this action regarding your credit. You are the best judge in determining irregularities in your credit report.

Q: What do I do now that I have my credit reports?

A: Review all sections on the credit reports carefully and highlight all incorrect information. Take note of any inaccuracies in all sections. The important fields are names, addresses, accounts and inquiries. The following sections, as described below, may vary from CRA to CRA.

- **First section**: this is personal identifying information which includes name, address, employment records, and Social Security Number and spouse's name.
- **Second section**: Credit account information which includes all credit cards and collection notices for the past seven years, whether active or not. This is where fraudulent credit cards currently being used will be listed.
- **Third section**: this is a list of application inquiries initiated by the consumer for the purposes of credit. This is where you find pending applications that are currently being processed.
- **Fourth section**: this is a list of companies that are considering you for pre-approved credit card offers. Consumers need not be concerned by this list.
- **Fifth section**: Includes any consumer statements and fraud alert

Q: How often should I review my credit reports?

A: Under Federal law, you are entitled to receive a free copy of a credit report from each of the three CRAs. This report is not in any way associated with the free report from placing a fraud alert. It is strongly suggested that you request your free copy of your credit report every four months. You should stagger these requests to the three credit reporting agencies throughout the year. This can be done using the free annual credit report program:

www.annualcreditreport.com or (877) 322-8228

Q: I've noticed inaccuracies on my credit reports. What should I do?

A: Contact the specific credit reporting agency (with the confirmation number and phone number provided on the report) to discuss the questionable content on the credit report.

If it is determined that this is more than just an inaccuracy, for further assistance, contact the LOSFA's call center at **1 (800) 259-5626, Ext. 1012.**

Q: What should I be on the lookout for?

A: Once you've taken the precautions of placing a fraud alert and requesting a credit report, watch for signs that your information is being misused.

For example:

- Bills or statements for unrecognized accounts
- Receiving credit cards that you didn't apply for
- Communication from bank or retailers making reference to closed account or insufficient funds notices on closed account.

- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason
- Receiving calls or letters from debt collectors or businesses about merchandise or services you didn't buy
- Warrants for your arrest
- Unexpected increase in pre-approved credit card offers
- Increase in insurance premiums
- Denial of credit, tenancy, job, or promotion
- Fraudulent activity or purchases you did not make on bank and credit card statements. Monitor them for any unexpected activity
- Missing bills, statements and/or mail. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter.

Q: What are the official websites for information about this situation?

A: The official website is http://osfa.la.gov

Additional Questions

Q: I'm a parent or guardian who co-signed on a savings account during the time frame involved. What do I need to do?

- Close the account and open a new one
- Request that the old account be flagged as "closed due to security breach"
- Request that the bank send a letter to the account holder verifying that the account has been closed and flagged.
- Password Protect New Accounts - a password should not be a mother's maiden name. A strong password should be more than 8 characters in length, and contain both capital letters and at least one numeric or other non-alphabetical character. Use of non-dictionary words is also advised.
- Place fraud alerts on your credit reports

Q: Do I need or can I get a new Social Security Number?

A: No. To change a Social Security Number requires a history of substantial misuse of that SSN. Changing a Social Security Number is a very serious step that should not be undertaken without a great deal of consideration and need.

Q: Will I be notified if anything that affects me changes? If so how?

A: Any changes in status will be posted on the website: http://osfa.la.gov. Any other communications from LOSFA will be sent by US Postal Service to your address of record. No one will be asking you for your Social Security Number or financial information.

If someone **does** ask for your Social Security Number then please notify the LOSFA Call Center: **1 (800) 259-5626, Ext. 1012.**

Q. Do I need a credit monitoring service?

A: Your fraud alert will warn you if someone is trying to apply for credit. You do not need to pay for credit monitoring since there is a federal *free annual credit report* program. This program allows you to get a free copy of your credit report once every 12 months from each Credit Reporting Agency. We recommend that you stagger your requests so that you get a report about every 4 months.

Note: The following section applies specifically to any one who might have been a minor during the years involved

Q. What if I don't have any credit?

A: Your credit report is only initiated when you first apply for credit. So, if you have never applied for credit, you **should not** have a credit report. That means you cannot place a fraud alert, since there is no credit file for the fraud alert to be placed against. However, it is recommended that you write the three credit reporting agencies to verify that there is no credit report in your name at this time. If one does exist, it will probably reflect no information other than your personal identifying information which includes name, address, employment records, and Social Security Number. For inquiries about child identity theft write to the following addresses:

Equifax:	**Experian:**	**TransUnion:**
P.O. Box 105069	PO Box 9532	PO Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834
		childidtheft@transunion.com

If, at this point, you find that there **is** a complete credit report with your Social Security Number, you need to contact the credit reporting agencies to dispute the reports, and also contact the LOSFA call center for further guidance.

Q. What is a credit report?

A: Your credit report is a factual record of your credit payment history as reported by your creditor. It includes your personal information, employment record, credit application inquiries, etc.

Q. What is a Credit Reporting Agency?

A: A Credit Reporting Agency (CRA) collects and distributes information about your financial and credit status, so that credit issuers can assess your credit worthiness. The three CRA's are Experian, Equifax, and TransUnion.