

***Flex*** Compensation, Inc.

P.O. Box 220  
Minneapolis, MN 55440-0220  
(952) 544-8332 (800) 333-5597

---

FAX COVER SHEET

DATE: February 25, 2007

TO: Office of Cyber Security & Critical Infrastructure Coordination  
Consumer Protection Board  
Office of the Attorney General, Bureau of Consumer Frauds

FAX #: 518-474-9090  
518-474-2474  
212-416-6003

FROM: Shannon Mealy-McCarthy, Mgr. Benefits Administration

RE: Your Check #14243166 payable to Flex Compensation, Inc.

PAGES: 9 (including cover sheet)

---

Reporting Form to advise of a security breach.

**Reporting Form  
For Business, Individual or NY State Entity reporting a  
"Breach of the Security of the System"  
Pursuant to the Information Security Breach  
and Notification Act (General Business Law §889-aa;  
State Technology Law §208)**

Name of Business, Individual or State Entity Flex Compensation, Inc.  
 Date of Discovery of Breach: February 14, 2007  
 Estimated Number of Affected Individuals: 63,400 (178 from State of NY)  
 Date of Notification to Affected Individuals: February 27, 2007  
 Manner of Notification:  written notice  
                                    electronic notice (email)  
                                    telephone notice

Are you requesting substitute notice?  Yes  No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

Laptop computer was stolen from office. Computer contained personal information such as Social Security number, name, address, and in limited cases, certain bank account information

Name of Business or Individual Contact Person: Shannon Mealy-McCarthy  
 Title: Mgr. Benefits Admin / Privacy Officer  
 Telephone number: 952-541-6333  
 Email: smealy@flexcompensation.com

Dated: February 25, 2007  
 Submitted by: Shannon Mealy-McCarthy  
 Title: Mgr. Benefits Admin / Privacy Officer  
 Address: P.O. Box 220, Minneapolis, MN 55440-0220  
 Email: smealy@flexcompensation.com  
 Telephone: 952-541-6333 Fax: 952-544-8287

**PLEASE SUBMIT THIS FORM TO ALL THREE (3) STATE AGENCIES as follows:**

**Fax** this form to the Office of Cyber Security & Critical Infrastructure Coordination (CSCIC) & Consumer Protection Board (CPB):

**CSCIC:**  
Security Breach Notification-  
fax: 518-474-9090

**CPB:**  
Security Breach Notification-  
fax: 518-474-2474

and also **Fax & Mail** this form to

**Attorney General:**  
Asst. AG in Charge  
Bur. of Cons. Frauds  
120 Broadway - 3<sup>rd</sup> Floor  
New York, NY 10271  
Fax No: 212-416-6003

**Flex Compensation, Inc.**

February 26, 2007

«fname» «lname»  
 «adr1»  
 «adr2»  
 «city», «st» «zip»

A laptop computer was recently stolen from the offices of Flex Compensation, Inc. (FCI). FCI provides employee benefit administration services for «orgname». You are receiving this letter because some of your personal information may have been included in the files on the computer.

We cannot determine precisely which participants' information was stored on the computer because the computer was not included in our daily back-up routine. Nevertheless, it is known that information stored on the computer included names, addresses, and Social Security numbers for some plan participants. It may also contain direct deposit banking information. The computer was used for troubleshooting system problems, testing system changes, and viewing historical data. Some of the information on the computer was several years old and may be incorrect and outdated.

We do not believe the thief knows that personal information is stored on the computer. If the thief does try to access information on the computer, he would have to circumvent the computer's security mechanisms, including logon and application passwords, to access the information. Nevertheless, we are providing this notice to alert you that your personal information could be accessed by the thief and used to commit fraud. This letter will explain the steps we have taken to protect against potential abuse of the information and will inform you of actions you can take to protect yourself.

**Actions We Have Taken**

Upon learning of the theft, we immediately notified law enforcement and building security. We have reviewed both the technical and physical safeguards in our operations and are making appropriate changes, including restricting access to its office building and suite, even while staff is still present. We have also performed an audit to ensure that no other participant data resides on any laptop or desktop machine that could be carried out of its office. In the past, downloading participant information onto laptops and workstations was restricted – it is now prohibited. Finally, we are reviewing the possibility of encrypting certain types of information.

**Actions You Should Take**

We don't believe there is reason to panic but here are some things to consider:

- You should closely monitor all financial statements such as your credit card accounts, checking and/or savings accounts, and then notify the appropriate institution if you notice any unauthorized activity. If you decide to close your bank account and you are currently enrolled for direct deposit through FCI, please notify us in writing.
- You can contact one of the credit agencies shown below to request a free credit file and/or request that a fraud alert be added to your file. It is our understanding that whichever agency you contact will automatically report your information to the other two agencies.

Credit Agency	Phone Number	Web Address
Equifax	800-685-1111 (for free credit file) 800-525-6285 (to report fraud)	<a href="http://www.equifax.com">www.equifax.com</a>
TransUnion	877-322-8228 (for free credit file) 800-680-7289 (to report fraud)	<a href="http://www.transunion.com">www.transunion.com</a>
Experian	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>

- Residents of many states may impose a credit freeze on their credit agency records. You should determine if you may impose such a freeze and decide whether you wish to direct the credit agencies to freeze your records.
- If you suspect unauthorized use of your Social Security number as it is related to employment or Social Security benefits, you can contact the Social Security Administration Fraud Hotline at 800-269-0271 to file a report.
- You should visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) to view the Federal Trade Commission's consumer education information.

We have contracted with Kroll Inc, to provide access to ID TheftSmart™ member services. If you have any questions about the incident, please contact them at 1-800-XXX-XXXX. Please reference **Coupon Number : XXXXXXXX** during the call. This is a special number that has been set up to assist you. Please do not call Flex Compensation's normal office number.

We deeply regret any inconvenience or concern the laptop theft may have caused you. Please be assured we are working together with our clients to minimize any ongoing impact of this incident.

Sincerely,

Gary A. Bohline  
President  
Flex Compensation, Inc.



February 26, 2007

«fname» «lname»  
 «adr1»  
 «adr2»  
 «city», «st» «zip»

A laptop computer was recently stolen from the offices of Flex Compensation, Inc. (FCI). FCI provides employee benefit administration services for «orgname». You are receiving this letter because some of your personal information may have been included in the files on the computer.

We cannot determine precisely which participants' information was stored on the computer because the computer was not included in our daily back-up routine. Nevertheless, it is known that information stored on the computer included names, addresses, and Social Security numbers for some plan participants. The computer was used for troubleshooting system problems, testing system changes, and viewing historical data. Some of the information on the computer was several years old and may be incorrect and outdated.

We do not believe the thief knows that personal information is stored on the computer. If the thief does try to access information on the computer, he would have to circumvent the computer's security mechanisms, including logon and application passwords, to access the information. Nevertheless, we are providing this notice to alert you that your personal information could be accessed by the thief and used to commit fraud. This letter will explain the steps we have taken to protect against potential abuse of the information and will inform you of actions you can take.

#### **Actions We Have Taken**

Upon learning of the theft, we immediately notified law enforcement and building security. We have reviewed both the technical and physical safeguards in our operations and are making appropriate changes, including restricting access to its office building and suite, even while staff is still present. We have also performed an audit to ensure that no other participant data resides on any laptop or desktop machine that could be carried out of its office. In the past, downloading participant information onto laptops and workstations was restricted – it is now prohibited. Finally, we are reviewing the possibility of encrypting certain types of information.

#### **Actions You Should Take**

We don't believe there is reason to panic but following are some things to consider:

- You should closely monitor all financial statements such as your credit card accounts, checking and/or savings accounts, and then notify the appropriate institution if you notice any unauthorized activity.
- You can contact one of the credit agencies shown below to request a free credit file and/or request that a fraud alert be added to your file. It is our understanding that whichever agency you contact will automatically report your information to the other two agencies.

Credit Agency	Phone Number	Web Address
Equifax	800-685-1111 (for free credit file) 800-525-6285 (to report fraud)	<a href="http://www.equifax.com">www.equifax.com</a>
TransUnion	877-322-8228 (for free credit file) 800-680-7289 (to report fraud)	<a href="http://www.transunion.com">www.transunion.com</a>
Experian	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>

- Residents of many states may impose a credit freeze on their credit agency records. You should determine if you may impose such a freeze and decide whether you wish to direct the credit agencies to freeze your records.
- If you suspect unauthorized use of your Social Security number as it is related to employment or Social Security benefits, you can contact the Social Security Administration Fraud Hotline at 800-269-0271 to file a report.
- You should visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) to view the Federal Trade Commission's consumer education information.

We have contracted with Kroll Inc, to provide access to ID TheftSmart™ member services. If you have any questions about the incident, please contact them at 1-800-XXX-XXXX. Please reference **Coupon Number : XXXXXXXX** during the call. This is a special number that has been set up to assist you. Please do not call Flex Compensation's normal office number.

We deeply regret any inconvenience or concern the laptop theft may have caused you. Please be assured we are working together with our clients to minimize any ongoing impact of this incident.

Sincerely,

Gary A. Bohline  
President  
Flex Compensation, Inc.

**Flex Compensation, Inc.**

## **Security Breach Questions & Answers**

---

### **1. Why did I receive the security breach notification letter?**

A computer was stolen from Flex Compensation, Inc. (FCI) that contained confidential personal information including Social Security numbers for participants in certain employee benefit plans administered by Flex Compensation.

### **2. What personal information was on the stolen computer?**

The computer may have contained the following confidential personal information:

- For individuals enrolled in COBRA continuation coverage it may have included name, address, birth date, Social Security numbers, and dependent information if you had family coverage.
- For individuals enrolled in the Health Care or Dependent Care Reimbursement accounts, it may have included the above information and bank account information for participants who were enrolled in direct deposit.

We don't believe the thief knows that there is confidential information on the machine, and accessing the information would require circumventing the computer's security including logon and application passwords. However, the data was not encrypted and therefore could be accessed by somebody with technical computer skills. We therefore feel it is important to notify individuals who may be at risk.

### **3. Who is Flex Compensation?**

Flex Compensation provides benefit administration services to employers and union groups. Services provided include reimbursement account administration for flexible spending account and health reimbursement arrangements, billing for benefit continuation following termination of employer provided coverage and benefit enrollment services. If you received the notice you are either currently employed by one of FCI's clients, or were formerly covered by a benefit plan sponsored by one of FCI's clients.

### **4. What specifically happened?**

On February 14, 2007 it was discovered that a laptop computer was stolen from Flex Compensation's office.

### **5. What is being done to recover the computer?**

The local police and the office building's security company were notified immediately. The police are working on the case and we have also offered a reward for the return of the computer.

### **6. Can you tell if my personal information was included?**

It is difficult to determine precisely which participants are involved. We developed to the best of our ability a list of individuals that we believe were on the machine. If you received a notification letter you were on that list.

### **7. What can I do to protect myself from identity theft and fraud?**

We don't believe there is reason to panic but following are some things to consider:

- You should closely monitor all financial statements such as your credit card accounts, checking and/or savings accounts and then notify the appropriate institution if you notice any unauthorized activity.

**Flex Compensation, Inc.**

### Security Breach Questions & Answers

---

- You can contact one of the credit agencies shown below to request a free credit file and/or request that a 90 day fraud alert be added to your file. It is our understanding that whichever agency you contact will automatically report your information to the other two agencies.

Credit Agency	Phone Number	Web Address
Equifax	800-685-1111 (for free credit file) 800-525-6285 (to report fraud)	<a href="http://www.equifax.com">www.equifax.com</a>
TransUnion	877-322-8228 (for free credit file) 800-680-7289 (to report fraud)	<a href="http://www.transunion.com">www.transunion.com</a>
Experian	888-397-3742	<a href="http://www.experian.com">www.experian.com</a>

- If you suspect unauthorized use of your Social Security number as it is related to employment or social security benefits, you can contact the Social Security Administration Fraud Hotline at 800-269-0271 to file a report.
- You should visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) to view the Federal Trade Commission's consumer education information.

#### **8. What actions has Flex Compensation taken to ensure that this security breach does not happen again?**

Flex Compensation takes data security very seriously and has developed policies and procedures to ensure the confidentiality of individual's personal information. As a result of this incident, we have reviewed both technical and physical safeguards and made appropriate changes.

#### **9. Will FSA or COBRA processes be affected for current participants?**

Flexible Spending Account claim payments will continue to be processed on the regularly scheduled dates, and direct deposits should post accordingly. COBRA payment processing will also continue as in the past. If you decide to close your bank account and you have elected direct deposit for FSA claim payments, you should notify us in writing. A direct deposit cancellation form is available on our website, [www.flexcompensation.com](http://www.flexcompensation.com), under Participant Resources.