

**North Carolina Security Breach Reporting Form  
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: Flex Compensation, Inc.  
Address: P.O. Box 220  
Minneapolis, MN 55440-0220  
Telephone: 952-541-6333  
Fax: 952-544-8287  
Email: slmealy@flexcompensation.com

**PLEASE SUBMIT FORM TO:**  
Consumer Protection Division  
NC Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
Telephone: (919) 716-6000  
Toll Free in NC: (877) 566-7226  
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: February 26, 2007  
Date the Security Breach was discovered: February 14, 2007  
Estimated number of affected individuals: 63,000  
Estimated number of NC residents affected: 682

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): \_\_\_\_\_

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: A laptop computer was stolen from our office, which contained personal information such as SSN, name, address, and in limited circumstances, banking information  
Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. YES If so, please describe the security measures protecting the information: Computer itself was password protected, as were the two software programs tha contained the personal information.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: systems have been audited to ensure that no personal info resides on machine that could be carried our of the office. Office is locked outside normal business hours even when staff are present

Date affected NC residents were/will be notified: February 27, 2007

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): n/a

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))  
 written notice  
 electronic notice (email)  
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.  telephone notice  
 substitute notice

Signature: SLM McCarthy Date: 2-26-07  
Contact Person, Title: Shannon Mealy-McCarthy, Mgr. Benefits Admin / Privacy Officer  
Address: \_\_\_\_\_  
(if different from above)  
Telephone: 952-541-6333 Fax: 952-544-8287 Email: slmealy@flexcompensation.com

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>

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>

February 26, 2007

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

Dear «fname»,

I am writing to inform you of an unfortunate incident involving some of your personal information. Our company, Flex Compensation, Inc., is the third-party administrator for COBRA continuation coverage and the Health Care and Dependent Care Reimbursement accounts sponsored by Client Name. On February 14, we discovered that a laptop computer had been stolen from our office.

You have been identified as one of the participants whose personal information may have been on the stolen computer. The personal information may have included your name, Social Security number, address, and in some limited cases bank account information. Although the information on the stolen computer is protected by two separate unique user identification numbers and passwords, we cannot be sure that someone will not access the personal information.

Protecting private information is a priority and a responsibility that we take very seriously at Flex Compensation. We are very sorry that this criminal act happened and we are working with law enforcement to recover the computer.

We are committed to protecting the privacy of your personal information. We are also committed to doing all we can to prevent similar events from happening in the future. Specific steps we are taking include reviewing our policies related to handling participant information, examining our computer security programs and continued training of employees to safeguard participant information.

In addition, we are making every effort to help you and other participants minimize any potential consequences of this theft. To assist in this, Client Name has contracted with Kroll Inc. to provide access to ID TheftSmart™. You will have access to the following services for a twelve month period, free of charge, should you enroll by July 12, 2007:

- free credit monitoring,
- access to a fraud investigative team and restoration services,
- access to a call center to answer questions.

To enroll in this service, please contact ID TheftSmart member services at 1-800-XXX-XXXX and provide the following coupon number: XXXXXXXX

Again, we want to emphasize how deeply we regret that this incident has occurred. Our staff is committed to addressing any of your issues or questions, and we have prepared the following Questions and Answers for you. If you have any additional questions or need assistance, please contact ID TheftSmart member services at 1-800-XXX-XXXX by July 12<sup>th</sup>.

Sincerely,

Gary Bohline  
President, Flex Compensation

## 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.

## 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.

**Flex Compensation, Inc.**  
www.flexcompensation.com

Mailing address: PO Box 220, Minneapolis, MN 55440-0220  
Street address: 600 S. Hwy 169, Suite 1570, St. Louis Park, MN 55426  
(952) 544-8332 (800) 333-5597 Fax: (952) 544-8287

February 26, 2007

Consumer Protection Division  
NC Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001

MAR - 5 2007

RE: Report of Security Breach

To Whom It May Concern:

This letter is in to advise that a laptop computer was recently stolen from the offices of Flex Compensation, Inc. (FCI). Flex Compensation provides benefit administration services to employers and union groups. We provide 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.

Enclosed please find the North Carolina Security Breach Reporting Form and copies of our notification to the affected individuals. Note that there are three different versions of the notice, so we have included all three for your records. A copy of this report was also faxed to your office today.

Please do not hesitate to contact either one of us if you have any questions or should you require further information regarding the incident.

Sincerely,

Gary Bohline, President  
President / Security Officer  
952-541-6335

Shannon Mealy-McCarthy  
Mgr. of Benefits Admin / Privacy Officer  
952-541-6333