

**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: Saint Vincents Catholic Medical Centers of New York ("SVC MC")  
Address: 153 W 11th Street  
New York, New York 10011  
Telephone: 212-604-7000  
Fax: 212-356-4990  
Email: contactus@svcmcnyc.org

**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:

October 15, 2007

Date the Security Breach was discovered:

June 1, 2007

Estimated number of affected individuals:

30,000

Estimated number of NC residents affected:

12

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:

On June 1, 2007, SVC MC learned that an employee transmitted electronic copies of certain SVC MC databases containing insurance-related information to his home computer in February, 2007. There is the possibility that this employee may also have disseminated the databases to an individual not currently employed by or associated with SVC MC. The employee in question had authorization to access the databases as part of his job responsibilities; however, he was not authorized to transmit the databases outside the control of the hospital. At this time, we have no knowledge of any misuse of this information beyond its unauthorized transmission.

We have found that certain mishandled databases contained insurance-related information concerning current and former patients, including, for example, name, date of birth, SVC MC account number, insurance carrier information, insurance claim information and insurance policy numbers. We do not believe that any medical information (such as diagnosis, treatment or medications) was included in these databases. Similarly, we do not believe that the databases contained any credit card or bank account numbers. However, some Social Security numbers were included in the mishandled databases, as insurance carriers sometimes use all or part of Social Security numbers as insurance policy numbers.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. No If so, please describe the security measures protecting the information:

Describe any measures taken to prevent a similar Security Breach from occurring in the future:

Reviewed the security settings on computers to prevent the use of unauthorized programs, and installed new, more effective tools to detect any unauthorized software installed on SVCMC workstations. Updating the roles of key IT security personnel and developing additional strategies to promote a secure data environment at SVCMC.

---

Date affected NC residents were/will be notified:

Notifications began mailing on October 12, 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):

Upon the discovery of this security breach, we promptly reported it to the local police department, who in turn began an investigation. To avoid any possible interference with its investigation, the District Attorney's office of the County of New York requested that SVCMC refrain from making its notifications required by state law. On September 23, the District Attorney's office granted SVCMC permission to proceed with its notifications.

**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.**

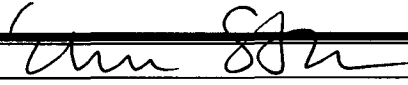
Please see attached

How NC residents were/will be notified?  
(pursuant to N.C.G.S. § 75-65(e))

**Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.**

- written notice  
 electronic notice (email)  
 telephone notice  
 substitute notice

---

Signature: 

Date: 10/15/07

Contact Person, Title: Elizabeth St. Clair, Esq. Senior Vice President, Chief Legal Counsel

Address:

(if different from above)

Telephone: (212) 604-8824

Fax: (212) 356-4990

Email: estclair@svcmcnyc.org



Saint Vincent  
Catholic Medical  
Centers

October 10, 2007

Dear Valued Patient,

I am writing to let you know about a recent incident involving insurance information held by Saint Vincents Catholic Medical Centers of New York ("SVCMC").

On June 1, 2007, SVCMC learned that an employee transmitted copies of certain SVCMC databases containing insurance-related information to his home computer in February, 2007. There is the possibility that this employee may also have disseminated the databases to an individual not currently employed by or associated with SVCMC. The employee in question had authorization to access the databases as part of his job responsibilities; however, he was not authorized to transmit the databases outside the control of the hospital.

**At this time, we have no knowledge of any misuse of this information beyond its unauthorized transmission.** However, we wanted to inform you about this incident so that you can best determine what steps you would like to take, if any.

Upon the discovery of this security breach, SVCMC promptly reported it to the proper law enforcement authorities, which in turn began an investigation. To avoid any possible interference with its investigation, the Manhattan District Attorney's office requested that SVCMC refrain from notifying individuals whose information may have been involved.

Independently, we engaged outside computer forensic experts to help us determine what information was contained in the databases and the exact nature and scope of the improper transmission of information outside the control of SVCMC. Although the forensics analysis is ongoing, we have found that certain mishandled databases contained insurance-related information concerning current and former patients, including, for example, name, date of birth, SVCMC account number, insurance carrier information, insurance claim information and insurance policy numbers.

**We do not believe that any medical information (such as diagnosis, treatment or medications) was included in these databases. Similarly, we do not believe that the databases contained any credit card or bank account numbers.** Together with our outside security experts, we will continue to investigate this matter thoroughly.

During our review of this incident, we determined that your insurance information was included in the compromised databases, and that, to the best of our knowledge, your insurance carrier had used all or part of your (or a family member's) Social Security number as part of its system to identify you.

SVCMC has notified your insurance carrier directly about this situation. Your carrier may elect to take measures to prevent unauthorized individuals from filing claims under your policy. We also recommend that you contact your insurer to inquire about any recent claims that have been made using your policy number.

#### **Credit Monitoring Offer and Other Precautionary Measures**

Because we have determined that all or part of your Social Security number was included in the compromised databases, SVCMC is offering to assume the cost for one year of credit monitoring. We have arranged for ConsumerInfo.com, Inc., an Experian company, to provide you with this membership at no cost to you. Experian's credit monitoring product is designed to identify and notify you of key changes in your credit reports that may indicate fraudulent activity. Detailed information about the credit monitoring membership is available at <http://partner.consumerinfo.com/svcmc>.

**Important Note:** Due to New York state law restrictions, identity theft insurance coverage cannot, by law, be offered by Experian to residents of New York. If you are a resident of New York state, please be aware that Experian's credit monitoring products will not include identity theft insurance, but will otherwise provide services as described by Experian.

You have until January 25, 2008, to activate your credit monitoring membership. To activate your membership, visit <http://partner.consumerinfo.com/svcmc> and enter the access code provided on the top of this letter. This web site will provide further instructions for registration. If you are unable to register or receive notifications online, you can instead use this access code to register for the offline version of Experian's credit monitoring service, by calling 1-888-898-0087.

Whether or not you choose to accept our offer of free credit monitoring, there are a number of additional precautions that you may consider:

- **You may periodically request a free credit report.** Every consumer, whether or not their data has been involved in a security breach, can receive one free report every twelve months from each of the three national credit bureaus listed below. You should remain vigilant about suspicious activity and check your credit reports periodically over the next 12 to 36 months.
- **You may place a fraud alert on your credit file.** A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. To place a fraud alert on your credit file, contact one of the three national credit bureaus at the numbers provided below.
- **In some states, you have the right to put a “credit freeze” on your credit file,** so that no new credit can be opened under your credit file without the use of a PIN number that is issued to you when you initiate your credit freeze. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit bureaus below to find out more information.

To order free credit reports from each of the three national credit bureaus, you can call the numbers below, or you can visit their websites for further contact information:

- Equifax (800) 685-1111 [www.equifax.com](http://www.equifax.com)
- Experian (888) 397-3742 [www.experian.com](http://www.experian.com)
- TransUnion (877) 322-8228 [www.transunion.com](http://www.transunion.com)

You should know that as a precaution, SVCMC will never ask you to provide any sensitive personal information, such as your Social Security number, except when you have placed a call to us, or through written requests mailed to your home or billing address. If you do happen to receive a telephone or e-mail contact with such a request, it is not from SVCMC and you should not provide any such information.

SVCMC takes the privacy and security of your personal information very seriously. While an incident like this is an unfortunate reality in today’s world, we are taking appropriate steps to reduce the chance of any future incidents like this at SVCMC. Specifically, we have reviewed the security settings on our computers to prevent the use of unauthorized programs, and installed new, more effective tools to detect any unauthorized software installed on SVCMC workstations. We are also updating the roles of key IT security personnel and developing additional strategies to promote a secure data environment at SVCMC. We truly regret that this incident occurred.

If you have additional questions or concerns, please feel free to call us at 1-866-675-3853, or you can read the Frequently Asked Questions (FAQs) that we have posted on our web site at <http://www.svcmc.org>.

Sincerely,

Michael Calder  
Senior Vice President