

**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: Celgene Corporation ("Celgene")
Address: c/o Brian Gill, Vice President, Corporate Communications
86 Morris Avenue
Summit, NJ 07901
Telephone: (908) 673-9530
Fax: (908) 673-2771
Email: bgill@celgene.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: August 15, 2007
Date the Security Breach was discovered: Celgene discovered the breach on July 24, 2007
Estimated number of affected individuals: Approximately 1,951
Estimated number of NC residents affected: Approximately 10

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 July 24, 2007, Celgene learned that four external computer hard drives used to back up information were missing from a locked Information Technology ("IT") workroom at its Summit, New Jersey offices. The IT workroom required keycard access to gain entry. Celgene immediately contacted the Summit, New Jersey police department and completed a police report. The police report number is 07-015072. Celgene also promptly began an investigation into the possible theft and to determine what information was on the external hard drives. Celgene determined that the hard drives contained personal information about its current and former employees, including name, address, phone number, social security number, date of birth, bank or other financial account information, compensation information, and in some instances, driver's license numbers. Celgene's investigation into this incident is continuing and includes the hiring of a reputable independent computer forensics and investigations firm. Attached is a copy of the notice to affected individuals.

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: Celgene will work diligently to improve IT and Security policies and procedures.

Date affected NC residents were/will be notified: Notices mailed on August 13, 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): After discovering the breach, Celgene undertook an internal investigation, including hiring a reputable computer forensics and investigations firm to determine what information may have been compromised, before notifying affected individuals.

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))

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: August 15, 2007

Contact: Timothy P. Tobin, Proskauer Rose LLP, on behalf of Celgene

Title: Attorney

Address: Proskauer Rose LLP
1001 Pennsylvania Avenue, NW
Suite 400 South
Washington, DC 20004

Telephone: 202-416-6870

Fax: 202-416-6899

Email: ttobin@proskauer.com



August 13, 2007

RE: IMPORTANT NOTICE

Dear

We are writing to inform you of the possibility that some of your personal information may have been compromised. We deeply regret that this situation occurred and are keenly aware of how important your personal information is to you. We do not yet have any knowledge that your information has been, or even is likely to be, misused. Nonetheless, we want to inform you of the incident and recommend some steps you can take to protect yourself from identity theft both now and in the future.

On July 24, 2007, we learned that four external computer hard drives used to back up information were missing from a locked Information Technology ("IT") workroom at our Summit, New Jersey offices. The IT workroom required keycard access to gain entry. We immediately contacted the Summit, New Jersey police department and completed a police report. Additionally, we then hired an independent computer firm specializing in forensics and investigations of this nature. This firm assisted in promptly beginning an investigation into the possible theft and determining what information was on the external hard drives. Although our investigation is ongoing, we have determined that two of the four hard drives contained personal information about our current and former employees that we possessed in our computer systems as of December 12, 2006. Celgene Corporation had this information about you for human resources purposes related to your employment and it resided among the business systems contained on these drives. Unfortunately, the personal information on the hard drives included, but may not have been limited to, your name, address, phone number, social security number, date of birth, bank or other financial account information, compensation information, and in some instances, driver's license numbers.

Again, although our investigation remains ongoing, we wanted to advise all employees and former employees of the information we have at this time. We also want to assist you in initiating efforts to minimize any potential identity theft. Indeed, we cannot be certain at this time whether the missing hard drives were unintentionally disposed of, taken for the values of the hard drives themselves rather than the information contained on them, or even if such personal information was viewed. As such, we emphasize again that we have no knowledge of any misuse of your personal information. Nevertheless, we want to help minimize the risk to you from this unfortunate event. We have arranged for you to enroll, at your option, free of charge for one year, in a credit-monitoring program sponsored by Equifax. The program will provide you with an early warning system for changes to your credit file and help you to understand the content of your credit file at Equifax. To enroll, follow the instructions on the enclosed page containing information about Equifax Credit Watch™ Gold.

August 13, 2007

Page 2

Whether or not you sign up for the Equifax credit monitoring program, it is always good practice to regularly review activity on your accounts and to obtain your credit report from one or more of the national credit reporting companies. You should contact the institutions where you hold financial accounts and let them know of the incident so they can notify you of any suspicious behavior or take other steps to protect you. We recommend that you remain highly attentive for at least the next 24 months and that you report any incidents of suspected identity theft to us and to proper law enforcement authorities. **We are also attaching a reference guide to give you more information on identity theft, how to report it and how to protect yourself.**

We have also established a hotline to address questions or concerns you may have. If you want to speak with someone at Celgene about this incident, please contact us toll free at 800-931-8681.

We sincerely apologize for this unfortunate event. Please know that we take this incident very seriously and as a result will work diligently to improve our IT and Security policies and procedures. We remain committed to protecting your personal information.

Sincerely,



Mary Weger
Corporate Vice President, Human Resources

Enclosures