



One CA Plaza  
Islandia, NY 11749

T +1 800 225 5224  
ca.com

July 16, 2008

**VIA OVERNIGHT MAIL**

Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: CA, Inc. – Notification of Potential Security Breach under N.H. Rev. Stat. §§ 359-C:19 et seq.**

Dear Attorney General:

We write to advise you of an incident in which a file containing certain personal information of former employees of Netegrity, Inc. (a company acquired by CA in 2004), was possibly accessed by an unauthorized party. On May 26, 2008, a break-in and theft occurred at the offices of Colt Express Outsourcing Services, Inc., a company that provided benefit plan administration services to Netegrity.

To our knowledge, an Excel file containing personal information as defined under state statute of a total of 973 individuals (507 former Netegrity employees and their dependents), only 42 of whom are New Hampshire residents. The information in the report that was potentially accessible included names, addresses, phone numbers, dates of birth, and Social Security numbers of these former Netegrity employees and their dependents. Apparently, the data of other employers was taken as well, the details of which we do not know.

**Learning About the Incident.** The incident involves a company called Colt Express Outsourcing Services, Inc., which was a benefit plan administration outsourcer to Netegrity, Inc. CA was advised by letter dated June 4, 2008 that on May 26, 2008, between approximately 4:30pm and 5:00pm PST, someone broke into Cold Express's office at 2125 Oak Grove Road, Suite 210, Walnut Creek California. Upon discovery the next morning, the incident was reported to the Walnut Creek Police Department, which filed report number 08-12367.

**Investigating the Incident.** We made several attempts to contact Colt to obtain more information about the incident but Colt continuously refused to provide any details of the incident because of an ongoing police investigation. When we contacted the Walnut Creek Police Department on June 25th, we were told that a server containing employee personal information of various companies was stolen. The police would not speculate as to whether the burglary was performed for purposes of obtaining identity theft data or committing fraud, but they indicated that only one individual had reported a claim relating to compromised credit.

As of this time, CA has no first hand knowledge that any employee information was misused as a consequence of the breach, and we are unaware of any reported instance of fraud or misuse of the data other than the one individual identified by the Walnut Creek Police related to this incident. We do not know whether the individual who reported the compromised credit was a Netegrity employee or an employee of another company also affected by this incident.

**Communicating with Affected Individuals.** In order to ensure that affected individuals could take immediate steps to protect themselves from possible identity theft or other harm or damage, CA will promptly notify them of the incident by sending notices via first-class mail on or about July 21, 2008. The notification letter, attached to this letter as Exhibit A, will, among other things, advise those former and current Netegrity employees and dependents to remain vigilant by reviewing account statements and monitoring free credit reports. The letter will also advise affected individuals that CA has procured on their behalf one year of Equifax's Credit Watch Gold Monitoring Services, and will further advise that them of their rights under law.

**Efforts to Prevent Reoccurrence.** CA has implemented steps to ensure that appropriate security measures are in place to prevent this kind of loss, to the extent it can be prevented. Some of these steps include formal policies, procedures and required employee training surrounding privacy and data protection to educate employees of their obligations with respect to the treatment of data; the implementation of a formal vendor questionnaire that is submitted to vendors before engaging with them to ensure that they have appropriate security procedures in place; the requirement that vendors sign a Data Protection Agreement which includes, among other things, requirements for data encryption and restrictions on data transfers; an internal process for ensuring that any sensitive data transferred to and from vendors is either encrypted or sent through secure means. We are currently implementing processes to audit these vendors on a periodic basis.

We trust that this letter and its enclosure provide you with all the information required to assess this incident and the adequacy of CA's response. Please let us know if you have additional questions or if we can be of further assistance. I can be reached at the telephone number and email address below my signature.

Sincerely,



Bonnie L. Yeomans  
VP and Privacy Officer  
Phone: (631) 342-2678  
Email: [bonnie.yeomans@ca.com](mailto:bonnie.yeomans@ca.com)  
Enclosure

## LETTERHEAD

July 21, 2008

[Field]

[Field]

Dear [Field]:

As a former employee or dependent of an employee of Netegrity (a company acquired by CA in 2004), we are writing you to let you know that your personal information, including name, address and Social Security number, may have been subject to unauthorized access or acquisition as a result of a break-in and theft of computers at the offices of one of Netegrity's external benefit administration vendors. If you are a former Netegrity employee, and Netegrity provided benefits to your dependents, the personal information of your dependents may also have been exposed by this incident. We are notifying all affected dependents who are 18 years of age or over under separate cover. Information about minor dependents can be found on the Equifax enrollment page enclosed with this letter. While we have no evidence that your personal information has been accessed or misused, we want to make you aware of the incident and the steps you should take to guard against identity fraud. If you are a current CA employee, please note that this incident does not affect your CA benefits in any way.

### **Credit Monitoring Services**

We have arranged with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you. The steps to follow are:

- i. Enroll in Equifax Credit Watch™ Gold. **CA has paid the fees for this service, and it is being provided to you at no cost for one year.** See the enclosed instructions for Equifax's simple internet-based verification and enrollment process.
- ii. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two credit reporting agencies, TransUnion and Experian.

Equifax Credit Watch™ Gold Monitoring will provide you with an "early warning system" to alert you to any changes to your credit file and help you to understand the content of your credit file at the three major credit reporting agencies. The key features and benefits of Equifax Credit Watch are as follows:

- i. Comprehensive credit file monitoring of your Equifax credit reports with daily notification of any key changes to your credit file;
- ii. Wireless alerts and customizable alerts are available;
- iii. \$20,000 in identity theft insurance with \$0 deductible, at no additional cost to you [†]; and
- iv. 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.

### **Directions for Placing a Fraud Alert**

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com) or contact Equifax's auto fraud line at 1-877-478-7625 and follow the simple prompts.

### **Where You Can Go For More Information**

If you want to learn more about identity theft, visit the following helpful websites:

- The Federal Trade Commission runs the U.S. government's identity theft information website, <http://www.consumer.gov/idtheft>. You can also contact the Federal Trade Commission via phone at 1-877-ID-THEFT (877-438-4338).
- The Identity Theft Resource Center is a non-profit organization that you can contact online at <http://www.idtheftcenter.org/> or via email to [itrc@idtheftcenter.org](mailto:itrc@idtheftcenter.org).

### **What Are Your Other Rights?**

We recommend that you carefully monitor all of your account statements. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. A free copy of your credit report may be obtained by contacting any one of the following national consumer reporting agencies:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion (FVAD)  
P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)

We apologize for any inconvenience. Even though CA's systems were not affected by this incident, we want you to know that CA takes the security of your personal data very seriously, and we are committed to minimizing the risks associated with the exposure of your personal information. The security of your information is of paramount importance to CA, and we maintain numerous safeguards to protect your information.

**For information about the free credit monitoring services we have arranged for you, please contact Equifax at 1-866-937-8432.** You may also contact CA's service desk for more information at 1-866-514-4772.

Sincerely,

Bonnie L. Yeomans  
VP and Privacy Officer

[†] Identity Fraud Expense Reimbursement Master Policy underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on underwriting qualifications and state regulations. Coverage not available for residents of New York. This product is not intended for minors (under 18 years of age). Equifax's credit monitoring products are protected by US Patent.

Netegrity NH AG

## **EQUIFAX CREDIT WATCH GOLD MONITORING ENROLLMENT INSTRUCTIONS**

Visit: [www.myservices.equifax.com/gold](http://www.myservices.equifax.com/gold).

- **Consumer Information:** Complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.
- **Identity Verification:** Complete the form with your Social Security Number, date of birth, telephone numbers, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.
- **Payment Information:** During the "check out" process, **provide the following promotional code: <XXXXXX>** in the "Enter Promotion Code" box. (no spaces, include dash.) After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)
- **Order Confirmation:** – Click "View My Product" to access your Credit Report and other product features.

To sign up for US Mail delivery of the product, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Promotion Code:** You will be asked to enter your promotion code as shown above (no spaces, **no dash**).
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax can not process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided).

### **MINORS (UNDER 18 YEARS OF AGE) AND EQUIFAX CREDIT WATCH**

Minors typically do not have a credit file, which is required for enrollment in the Equifax Credit Watch product. However, to give parents/guardians peace of mind that their child does not have a credit file they can take the following actions.

- 1) Try to place a fraud alert on the child's credit report. Call 1-877-478-7625. The system will ask for Social Security Number and address information. If the system responds by asking for additional id verification documents such as SSN card, then this confirms that the child does not have a credit file.
- 2) Search your child's credit file-at [www.annualcreditreport.com](http://www.annualcreditreport.com). Enter the child's information. If the system responds by asking for additional id verification documents such as SSN card, then this confirms that the child does not have a credit file.
- 3) Parents/guardians can send a copy of the minor child's birth certificate and a copy of a social security number card or letter/form from the Social Security Administration along with a letter explaining that they may be a victim of identity theft. Additionally, please provide a copy of your driver's license or other government-issued proof of your identity, which includes your current address. Please send this information to the following address:

Equifax Information Services  
P.O. Box 740256  
Atlanta, Georgia 30374

Once Equifax receives this information, it will perform a search of its database for a credit file under the child's SSN number. If Equifax does NOT find a match, then Equifax will inform the parent or guardian in writing that a credit file was not found.