Attachment A
Notice to New York Residents

December 22, 2005

[FirstName] [LastName]
[Address]
[City], [State] [ZIP]

Dear [FirstName] [LastName]:

Recently we mailed you a free copy of our software. We believe that this complimentary software will meet your 2006 tax preparation needs, based on our prior experience with you as an client. We hope that you will try and find it to be a great solution for filing your next tax return.

However, since we originally sent you this CD, we have become aware of a mail production situation that has affected a small percentage of recipients, including you. Due to human error in developing the mailing list, the digits of your social security number (SSN) were used as part of your mailing label's source code, a string of more than 40 numbers and characters. Fortunately, these digits were embedded in the middle of the string, and they were not formatted in any manner that would identify them as an SSN.

Nevertheless, we sincerely apologize for this inadvertent error, which is completely inconsistent with our strict policies to protect our clients' privacy. Our internal policies limit the use of client SSNs for purposes other than tax preparation. Furthermore, our internal procedures require that mailing source codes are formulated in a manner that excludes use of any sensitive or confidential information. Please know that we have conducted a thorough internal review of this matter, and are taking actions to ensure this does not re-occur.

Again, please understand that the digits of your SSN were embedded in the middle of a lengthy source code, and they were not formatted in a manner that identifies them as an SSN. As a result, we believe the exposure of your SSN digits was limited to you alone, since you are the only person who would recognize their significance. Nonetheless, we suggest that you destroy the wrapper and mailing label of the free CD we sent you. If you would like more information about this incident, please visit www. , a special Website that contains additional details and an e-mail link for contacting us with your questions.

On behalf of the more than 100,000 associates of allow me to apologize for this unfortunate situation. Through 50 tax seasons, has earned a reputation as a valued, trustworthy ally to our clients, and we sincerely hope that you will find the free CD and our information-packed taxcut.com Website to be helpful tools for the 2006 tax filing season.

Sincerely,

Senior Vice President & General Manager

How could this letter be improved?

Information about breach in 1st paragraph.

February 10, 2006

We have received information that there has been a breach of our regional computer network. After careful evaluation, it has been determined that the breach was from a roving worm looking for a place to store and serve large files containing illegal movies and music. We are required under a recent law enacted in New York State known as the Information Security Breach and Notification Act to notify individuals if their private information may have been compromised. Private information can include account numbers and social security numbers.

We have no knowledge that any private information was obtained by unauthorized entities but we are taking the precautionary step of notifying you that the possibility exists.

We have taken the necessary steps to ensure that the affected servers have been cleaned and secured. We also have taken steps to ensure the security of private data in the future. However, we believe that it is important for you to continue the routine monitoring of your accounts for unusual activity. If you notice anything unusual, you should promptly contact your financial institution.

If you have any questions, you may contact us at between the hours of 9 AM and 3 PM, EST.

Sincerely,

District Superintendent & CEO

How could this letter be improved?

- written in Plain lang.
- info on what's been breached
- info on how to protect self.

recently has learned that a laptop of one of its employees was stolen during a burglary at . 's regional office in Atlanta, Georgia. This laptop contained personal information relating to certain current and former . personnel, such as social security numbers. Although this laptop was password-protected, some of your personal information, specifically your Social Security Number, may or may not have been contained on this laptop.

We currently have no reason to believe that the laptop was stolen for the information it contained, but rather for the laptop itself. For your own protection, however, you may wish to place a fraud alert on your credit file by calling one of the following three major credit bureaus:

Equifax	Experian	TransUnionCorp
800-525-6285	888-397-3742	800-680-7289

Additionally, you may wish to visit the Federal Trade Commission's web site, www.consumer.gov/idtheft, which contains information to help individuals guard against and deal with identity theft.

Please be assured that . is working with law enforcement on this matter and continues to take the protection of your information very seriously. Should you have any questions or comments, you may contact us as follows:

How could this letter be improved?

- date of breach
- date of discovery

4/27/2006

Dear Client,

The purpose for this letter, unfortunately, is to inform you that our office was burglarized. All our computers were stolen and we are actively working with law enforcement officials to investigate this matter. Although the computers are double password protected and there were no credit files stored on them, it is wise to take every precaution as there is the possibility that personal information may have been accessed. Inc is providing the following information to help protect you from potential misuse of your information including the potential of identity theft.

We recommend that you do the following:

▶ Add a security alert statement to your credit file at all three national credit reporting agencies, Trans Union, Equifax and Experian. The alert will remain on your credit file for 90 days. You only need to contact one of the three national credit reporting agencies below, your request will be shared electronically with the other two repositories. The most efficient method for doing this is to use the automated system provided by TransUnion by dialing 800.680.7289. (estimated time for completion is less than 3 minutes)
▶ Remove your name from pre-approved offers of credit mailing lists for approximately 6 months. The most efficient method for doing this is via website. The address is www.optoutprescreen.com and the process takes less than 2 minutes.
▶ Receive a free copy of your credit report. The most efficient method for doing this is via website at www.annualcreditreport.com or by calling (877) 322-8228.

The contact information for the three credit reporting agencies:

Equifax Credit Information Services Inc.
P.O. Box 740256
Atlanta, GA 30374
1.800.685.1111

TransUnion Credit Bureau
P.O. Box 2000
Chester, PA 19022
1.800.888.4213

Experian
P.O. Box 9554
Allen, TX 75013
www.experian/consumer
1.888.397.3742

You should also know that the Federal Trade Commission (FTC) offers consumer assistance and educational materials relating to identity theft and privacy issues. The FTC can be contacted by either visiting www.consumer.gov/idtheft or by calling (877) 438-4338.

We hope this information is helpful to you. We can be reached at 631-589-4215 if you have any questions about this information. We at Inc sincerely regret any inconvenience or concern this incident may cause.

Sincerely.

Vice President

How could this letter be improved?

- date of incident

To All Students and Staff,

On Friday Night May 21st, the administrative offices were broken into and several pieces of office equipment including a LCD projector, flat screen monitor and our central server were stolen. We met with the Santa Monica Police Saturday morning regarding the break-in and discussed our concerns including the possibility of identity theft.

Our server has an internal security system and is password protected. The police do not believe the nature of this break in corresponds to identity theft. Criminals involved in identity theft generally don't obtain information through high risk, physical break-ins that are immediately detectable.

As a precaution, please review the Privacy Rights Clearinghouse site at http://www.privacyrights.org. It provides useful information if any suspicious activity occurs with your credit. Again the police do not believe that this type of break in conforms to identity theft, however, please report any suspicious activity in accordance to the guidelines of the Privacy Rights Clearinghouse and also to us.

Our data is regularly backed up but additional restoration and verification will occur this week. To accommodate this, several delays will occur:

- Clinic Add/Drop will be delayed two days and begin on Wednesday at 10am in the library as usual.
- Student registration will begin as scheduled Tuesday June 1, at 10am in the library as usual.
- Any differences between scheduled and actual hours worked in the student clinic these last two weeks should be directed to Tim.

Additionally, greater security including surveillance cameras will be installed.

I realize that this may cause you some anxiety, but we are working with all possible speed to resume operations and enhance community safety. Thank you for your understanding. If you have any additional concerns, you may call or meet with me directly.

Chief Executive Officer

How could this letter be improved?

- date
- complete info on protection in the letter
- info on what was stolen

COLLEGE

January 6, 2006

[redacted]

We regret to notify you of a breach in our electronic security that resulted in your social security number being compromised by an intruder in our IT system. The breach resulted from the installation of a keystroke capture program on the desktop PC of a member of our staff at our unit. We have determined that the program was installed, unbeknownst to our employee, by a close relative in order to capture and read e-mail messages that the staff member was sending. The capture program was in operation from March 2004 to January 2005 and from October 2005 to December 15, 2005. We have removed the infected PC and are in the process of cleaning the hard drive of any and all virus and/or capture programs.

As required by the New York State Cyber Security Policy P03-02, we have notified the Consumer Protection Board, the New York State Office of Cyber Security and Critical Infrastructure Coordination, and the Attorney General, as well as the New York State Police.

Should you have any questions about this matter, please contact my office.

Sincerely,

Vice President for Administration

How could this letter be improved?

- information about how to protect yourself

Office of Administration •
phone