

USProtect

801 ROEDER ROAD.
SUITE 1000
SILVER SPRING, MD 20910
240-247-5068
FAX 240-247-5075

FACSIMILE TRANSMITTAL SHEET

TO: <i>Consumer Protection Board -</i>	FROM:
<i>Security Breach Notification</i>	Heather Cheyne
FAX NUMBER:	DATE:
<i>518-477-2474</i>	MAY 30, 2006
RE: <i>Security Breach Notification</i>	TOTAL NO. OF PAGES INCLUDING COVER: <i>6</i>

- URGENT
 FOR REVIEW
 PLEASE COMMENT
 PLEASE REPLY
 PLEASE RECYCLE

NOTES/COMMENTS:

Please do not hesitate to contact me if you require anything further.

Have a great day!

-Heather Cheyne
Director, Human Resources, USProtect

Law Firm

**Reporting Form
 For Business, Individual or NY State Entity reporting a
 "Breach of the Security of the System"
 Pursuant to the Information Security Breach
 and Notification Act (General Business Law §889-aa;
 State Technology Law §208)**

Name of Business, Individual or State Entity	<u>US Protect</u>
Date of Discovery of Breach:	<u>February 9, 2006</u>
Estimated Number of Affected Individuals:	<u>2 current NY residents</u>
Date of Notification to Affected Individuals:	<u>May 19, 2006 and May 24, 2006</u>
Manner of Notification:	<input checked="" type="checkbox"/> written notice
	<input type="checkbox"/> electronic notice (email)
	<input type="checkbox"/> telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

On or about March 13, 2006, US Protect Corporation ("US Protect") learned that a computer (the "Computer") was stolen from Snyder, Cohn, Collyer, Hamilton & Associates, P.C. ("Snyder"), an accounting firm retained by US Protect to conduct an audit of US Protect's 401(k) plan. Snyder informed US Protect that the computer may have contained personal information concerning US Protect's New York plan participants.

After conducting an investigation, Snyder believes that the perpetrator of this crime was interested in the value of the machine itself and was unaware of the data contained within the Computer. Access to that data required use of an access code which Snyder has no reason to suspect that the culprit has obtained. Snyder implemented the following responsive action plan:

- (1) On February 10, 2006, Snyder filed a report with local law enforcement alerting them of the theft.
- (2) On February 10, 2006, Snyder contacted the Computer's manufacturer and alerted them of the theft to ensure that the manufacturer did not assist the culprit in circumventing the Computer's access block.
- (3) On May 19, 2006 Snyder and US Protect voluntarily initiated a mailing to each New York resident potentially affected by this incident. The mailing (i) described the nature of the incident, (ii) described efforts taken to protect the recipients from any misuse of the data, (iii) advised the recipients to contact the three national credit reporting agencies and the New York Attorney General if they believe that they have been the victim of

identity theft, and (iv) directed the recipients to call Snyder with any additional questions. A copy of the notice is included as Attachment A.

US Protect respectfully requests that the information contained in this notice be kept confidential. Any details regarding this incident that are made public could jeopardize the security of the impacted individuals by notifying the perpetrator of this theft that the Computer may contain sensitive information.

Name of Business or Individual Contact Person: Katy Levine
US Protect Corporation
Title: Vice President & Controller
Telephone number: (240) 247-5311
Email: klevine@usprotect.com

Dated: May 26, 2006
Submitted by: Richard Norman
Title: President
Address: USProtect Corporation, 801 Roeder Rd., Suite 1000, Silver Spring, MD 20910
Email: rnorman@usprotect.com
Telephone: (240) 247-5066 Fax: (240) 247-5324

**SNYDER COHN COLLYER HAMILTON & ASSOCIATES P.C.**

May 16, 2006

CONFIDENTIAL

Dear USProtect 401(k) Account Holder:

Snyder, Cohn, Collyer, Hamilton & Associates, P.C. ("Snyder Cohn") has been hired by USProtect Corporation 401(k) Plan to provide accounting services for your retirement plan. In February, Snyder Cohn discovered that a computer which may have contained your social security number and date of birth was stolen.

Please be assured that we have no reason to suspect that your personal information has been accessed by an unauthorized individual. A security code is required to access any information contained on the stolen computer and Snyder Cohn has no reason to believe that the culprit knew of, or obtained, that code. Indeed, Snyder Cohn believes that the perpetrator of this crime was interested solely in the value of the machine itself and was unaware of the data contained within the computer.

Although we have no reason to suspect that your personal information, if it was on the computer, has been accessed by an unauthorized individual, Snyder Cohn is informing you of this event as requested by your plan administrators. We would like to also inform you that several steps have been taken to provide you with protection. Upon discovering the theft, Snyder Cohn immediately filed a report with local law enforcement alerting them of the incident. Snyder Cohn contacted the computer's manufacturer and alerted them of the theft to ensure that the manufacturer does not assist the culprit in circumventing the computer's access block.

In addition to the actions which have already been described, we would like to advise you to, as a precautionary measure, review your financial account statements and credit reports on a regular basis. You can obtain one free copy of your credit report per year from the three national consumer reporting agencies identified below. To order your free annual report from one or all of the companies, visit <http://www.annualcreditreport.com>, or call toll-free 877-322-8228.

Equifax 800-525-6285

Experian 888-397-3742

TransUnion 800-680-7289

Certified Public Accountants and Business Advisors4520 East West Highway, Suite 520, Bethesda, MD 20814-3338
Phone: 301-652-6700 Fax: 301-986-1028Web: cpahelp.com E-Mail: advice@cpahelp.com

Independent Member

BKR

Firm in Principal Cities Worldwide



If you determine that an account has been fraudulently established using your identity, you should call the national consumer reporting agencies above immediately as well as contact the Federal Trade Commission and your state attorney general's division of consumer protection, and advise them of any potentially fraudulent activity. Additional information about reporting, and preventing, identity theft can be found at <http://www.consumer.gov/idtheft>. We also have enclosed a Reference Guide to assist you in taking these precautionary steps.

On behalf of Snyder Cohn allow me to apologize for this unfortunate situation. Should you have further questions about this matter, do not hesitate to contact me at 301-652-6700.

Sincerely,

Mitchell G. Segal
Director of Operations
Snyder Cohn Collyer Hamilton & Associates, PC

REFERENCE GUIDE

While there is no indication that the data on the laptop has been misused, it is prudent to know about identity theft and what you can do to protect yourself.

About Identity Theft

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often times without your knowledge of the activity.

Identity Theft Prevention

You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may call any one of the three major credit reporting companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), complete name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; P O Box 740241, Atlanta, GA 30374-0241
Experian: 888-397-3742 www.experian.com; P O Box 9532, Allen, TX 75013
TransUnion: 800-680-7289 www.transunion.com; Fraud Victim Assistance Division, P O Box 6790, Fullerton CA 92834-6790

We recommend that you check your credit reports and review your account statements periodically. This can help you spot problems and address them quickly.

In addition, under federal law you are entitled to a free copy of your credit report, at your request, from each of the major nationwide credit reporting companies once every 12 months. To order your free annual credit report from one or all of the national credit reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Service, P O Box 105281, Atlanta, GA 30348-5281. You can print the form from www.ftc.gov/credit. If you ask, only the last four digits of your Social Security number will appear on your credit reports.

To learn more about how to protect yourself against identity theft, please visit www.consumer.gov/idtheft or call the Federal Trade Commission hotline phone number: 1-877-IDTHEFT (438-4338). You may call or visit the Federal Trade Commission Web site to report any incident of suspected identity theft.