



WHERE IDEAS MEET INDUSTRY

Douglas P. Hardy
Assistant General Counsel - Labor & Employment
SPX Corporation
13515 Ballantyne Corporate Place
Charlotte, NC 28277
Phone: 704-752-4524
Fax: 704-752-7511

April 15, 2008

Via First Class Mail and Facsimile (617-727-3265)

Honorable Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

RE: Data Breach Notification

Dear Attorney General Coakley:

Please be advised that on March 25, 2008, we received notice from one of our vendors, USinternetworking, Inc. (USi), that a USi laptop was stolen from the home of one of its employees. USi originally informed us that the laptop included personal identifying information, including names, Social Security numbers, and banking information, on approximately 329 individuals, 3 of whom reside in your state. We later received word from USi that an additional 74 individuals were affected by this incident, none of whom reside in your state. We attach copies of the notifications we received from USi.

Upon learning of this incident, in an effort to notify affected individuals as soon as possible, we forwarded a copy of the USi's March 25, 2008, communication to each of the affected individuals. See attached specimen copy of our cover memorandum.

On March 27, 2008, we received additional information from USi concerning the credit monitoring and identity-theft protection services USi would be making available to affected persons at its expense. We plan to begin forwarding this additional information to the affected individuals in the next several days. A draft copy of the supplemental notification that will be sent is attached.

As set forth in the attached letter, we have and continue to take steps to protect the security of the personal information. Also, in addition to continuing to monitor this situation, we are reexamining our current data privacy and security policies and procedures to find ways of reducing the risk of future data breaches. Should we become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

Douglas P. Hardy,
Assistant General Counsel - Labor & Employment

Encl.



An APV Company

USinternetworking, Inc.

ONE USI PLAZA

ANNAPOLIS, MARYLAND 21401-7478

TEL 410-897-4400

March 25, 2008

Via e-Mail and Federal Express

SPX Corporation
13515 Ballantyne Corporate Place
Charlotte, NC 28277

Re: Important Notice-Potential Exposure of Personal Identifying Information

Dear Valued Customer:

As discussed earlier today, this letter is to advise you of a recent theft of a laptop computer containing personal identifying information, including names, Social Security numbers, and banking information of approximately 329 employees of SPX Corporation who came from the APV acquisition.

The laptop was stolen from the home of a USi employee early Sunday morning, March 23, 2008. USi has reported the theft to law enforcement authorities and we believe the theft was a random act, based on the fact that other items, including a television set, were stolen from the home. The laptop was password protected and we have no evidence that your employees' personal information has been, or will be, used for unauthorized purposes. However, as a precaution, we are notifying you that the possibility exists that this information could be used to open or access your employees' credit or bank accounts.

Furthermore, USi is going to offer to your affected employees, free of charge, one year of credit monitoring and identity-theft protection. We expect to be able to provide you with further details later today or tomorrow regarding the protection plan.

Finally, we urge you to have your employees contact any of the major reporting agencies to place a fraud alert on their credit report and to notify their banks to change their bank account information. On the second page of this letter are details on how to contact the credit reporting agencies.

USi deeply regrets this incident and apologizes for any inconvenience this may have caused you or your employees. USi is taking steps to enhance the protection of the information you have entrusted to us to avoid future such incidents.



An AT&T Company

USinternetworking, Inc.

ONE USi PLAZA

ANNAPOLIS, MARYLAND 21401-7478

TEL 410-897-4400

Fraud Alerts

We suggest your employees contact the fraud departments of any one of the three major credit-reporting agencies and let them know you may be a potential victim of identity theft. That agency will notify the other two. Through that process, a "fraud alert" will automatically be placed in each of your three credit reports to notify creditors not to issue new credit in your name without gaining your permission. Contact:

Equifax

PO Box 740241
Atlanta, GA 30374
To report fraud, call:
1-877-478-7625
www.equifax.com

Experian

PO Box 2002
Allen, TX 75013
To report fraud, call:
1-888-397-3742
www.experian.com

TransUnion

PO Box 6790
Fullerton, CA 92834
To report fraud, call:
1-800-680-7289
www.transunion.com

We also encourage your employees to carefully review their credit report(s). Have them look for accounts they did not open or inquiries from creditors they did not initiate. They should also review their personal information for accuracy, such as home address and Social Security number. If they see anything they do not understand or that is inaccurate, call the reporting agency at the telephone number on the report. If they find suspicious activity on their credit reports or bank account(s), they should call their local police, file a police report of identity theft and get a copy of the report. They may need copies of the police report to clear their personal records.

SPX

13515 Ballantyne Corporate Place
Charlotte, NC 28277
866-779-2427
704-752-4400

March 25, 2008

(Name)
(Address)
(City, Street, Zip)

Dear (Name),

Further to verbal notices to employees of earlier today, we wanted to provide further information concerning a security incident that has occurred at one of our vendor sites, USi. USi provides payroll processing and data management services for SPX companies, and has been a trusted partner for many years.

USi has informed us that one of their employees was a victim of a home burglary. Multiple items were stolen, including a laptop containing some APV employee information, including 329 employee names, Social Security numbers, bank account and routing numbers and account type. Home addresses were not included. Please see the attached letter from USi, which provides further details about this incident and the measures USi is taking to manage it.

Also enclosed is important information about steps you can take to prevent misuse of your personal information. As stated in USi's letter, you will have access to one year of credit monitoring and identity-theft protection, at USi's expense. Details of this will be sent to you in the next couple of days. In addition, SPX has established a help line you can access at **(704) 752-7499** with questions or concerns.

We take this very seriously and we apologize for any inconvenience this incident may cause. We will continue to devote substantial resources toward managing it appropriately, and guarding against any similar incidents.



John P. Walsh, Jr.
Chief Information Security Officer



A. Michelle Brehm
Chief Data Privacy Officer



WHERE IDEAS MEET INDUSTRY

Douglas P. Hardy
Assistant General Counsel - Labor & Employment
SPX Corporation
13515 Ballantyne Corporate Place
Charlotte, NC 28277
Phone: 704-752-4524
Fax: 704-752-7511

[FIRST NAME] [LAST NAME]
[STREET ADDRESS]
[EXTENDED ADDRESS]
[CITY], [STATE] [ZIP]

Dear [FIRST NAME] [LAST NAME],

Over the past few weeks, we informed you that, USi, a service company that was doing information technology work for SPX to support human resources and payroll, notified SPX that USi experienced a data breach involving your personal information, including your name, address, Social Security number, and bank information. This letter is to notify you of the additional information referred to in our prior letter, including information about the credit monitoring and identity-theft protection services that would be made available to you at USi's expense.

To date, although we have no evidence that this information has been misused, because we take the possibility of identity theft very seriously, we want to provide additional information and tools to assist you in protecting your personal information and identity.

- USi has contracted with Kroll Inc. to provide you with access to its ID TheftSmart™ service. This service includes access to Continuous Credit Monitoring and Enhanced Identity Theft Restoration at no cost to you for 2 years. ID TheftSmart is a comprehensive program to help protect your name and credit against identity theft. We urge you to take the time to read about the safeguards now available to you. If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services at 1-800-588-9839 between 8:00 a.m. and 5:00 p.m. (Central Time), Monday through Friday.
- USi promptly reported the incident to law enforcement and an investigation is underway.
- The attached sheet provides additional information concerning steps you could take to protect your identity, credit and personal information.

We treat all sensitive employee information in a confidential manner and are proactive in the careful handling of such information. We currently are reviewing and assessing our existing privacy and data security policies and procedures to determine whether changes are needed to prevent similar situations from occurring.

Again, we apologize for any inconvenience this incident may cause you or your family. We encourage you to take advantage of the resources we have provided to you to protect your personal information.

Sincerely,

Douglas P. Hardy,
Assistant General Counsel – Labor & Employment

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
 - Add a security alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This security alert will remain on your credit file for 90 days.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
P.O. Box 740241
Atlanta, GA 30374
(877) 478-7625
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834
(800) 680-7289
www.transunion.com

2. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft and privacy issues. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

4. *For Massachusetts Residents:* You have the right to obtain a copy of the applicable police report relating to this incident. If you would like to request a security freeze be placed on your account, send all of the following (documentation for both the spouse and the victim must be submitted when requesting the spouse's credit report) to one or more of the credit-reporting agencies listed in item 1 above: full name, with middle initial and generation, such as JR, SR, II, III, etc.; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years. In addition, enclose one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., and one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible (enlarge if necessary), displays your name and current mailing address, and the date of issue (statement dates must be recent). The fee for placing a security freeze on a credit report generally is \$5. If you are a victim of identity theft or spouse of a victim of identity theft and submit a valid investigative or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles (DMV), the fee will be waived.
5. *For Maryland Residents:* The contact information for the State's Attorney General is

Honorable Douglas F. Gansler
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Website: <http://www.oag.state.md.us/>
Telephone number: (888) 743-0023
(toll-free in Maryland)