



X.L. Global Services, Inc.
Seaview House
70 Seaview Avenue
Stamford, CT 06902-6040
USA
Phone 203-964-5200
Fax 203-964-0763
www.xlcapital.com

April 16, 2008

Director
Office of Consumer Affairs and Business Regulation
Commonwealth of Massachusetts
Ten Park Plaza, Suite 5170
Boston, MA 02116

Office of the Attorney General
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108

Re: Notification of Security Breach

To Whom It May Concern:

In accordance with Massachusetts General Law Ch. 93H, I am writing to inform you about a security breach. A personal computer was recently stolen from an employee of one of our vendors, USInternetworking, Inc. of Annapolis, Maryland ("USi"). The personal computer contained the personal information of employees of XL Global Services Inc. or its affiliates ("XL"), including approximately 3 Massachusetts residents.

XL takes privacy and security matters very seriously. At our request, USi immediately reported the theft to local law enforcement in Columbus, Ohio to investigate the matter. However, the investigation has not yet been successful. We have sent multiple e-mail notifications to the affected employees to notify them of the breach and the status. We have also had the attached notice sent to all individuals (including Massachusetts residents) we have identified whose personal information may have been accessed by an unauthorized individual. The notices describe, among other things: (1) the general nature of the incident resulting in the potential information security breach, (2) the type of personal information that was the subject of the possible security breach, (3) the precautionary measures USi is taking (at XL's request) to help protect personal information from unauthorized use, (4) contact information for inquiries, and (5) how to enroll in Kroll's identity theft restoration and continuous credit monitoring services, which are being made available to affected by USi (at XL's request) to individuals free of charge for two years.

Please contact me if you require any additional information concerning this matter.

Sincerely,

Daniel J. Losito
Associate General Counsel
Enclosure



Secure Processing Center | 600 Satellite Blvd | Suwanee, GA 30024

Urgent Message from XL Global Services, Inc.
Please Open Immediately.

<FirstName> <MiddleInitial> <LastName> <Suffix>
<Address> (Line 1)
<Address> (Line 2)
<City> <State> <Zip>
<POSTNET BARCODE>

Re: Notice of Potential Disclosure of Personal Identifying Information and Information Regarding Identity Theft Safeguards to be provided by Kroll Inc.

Dear <FirstName> <MiddleInitial> <LastName> <Suffix>,

As you know from an email sent to you in March 2008, X.L. Global Services, Inc. (the "Company") was informed by one of our third party vendors, USInternetworking Inc. ("USi"), of the theft of a USi laptop computer containing personal identifying information, including yours. This information included names, addresses, and Social Security numbers of employees of the Company and its affiliates.

Although we have no evidence that this information has been improperly accessed or misused, we want to make you aware of the incident and the steps that have been taken to prevent a reoccurrence. USi management immediately reported the theft to law enforcement authorities, and USi has been actively cooperating with those authorities in the continuing investigation. USi has also informed us that the laptop itself was password protected and the two files containing the personal identifying information of Company employees would not be immediately evident.

Because protecting your personal information is so important to us, USi has engaged Kroll Inc., the world's leading risk consulting company, to provide with access to its ID TheftSmart™ service. This service includes Enhanced Identity Theft Restoration and Continuous Credit Monitoring at no cost to you for two years.

ID TheftSmart is one of the most comprehensive programs available 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 am and 5:00 pm (Central Time), Monday through Friday.

On behalf of USi and the Company, we sincerely regret this incident.

Very truly yours,

Richard Pikowski, Global Head of Human Resource Operations
X.L. Global Services, Inc.



<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-588-9839
8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services



<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-588-9839
8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services

Please detach cards and keep in a convenient place for your reference

U.S. State Notification Requirements

For residents of Hawaii, Maryland, Michigan, North Carolina, Oregon, Vermont, and Wyoming:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

Equifax
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

For residents of Oregon and Maryland:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland:

You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

For residents of Massachusetts:

It is required by state law that you are informed of your right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past two years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Consumer Credit Report and Credit Monitoring Authorization Form

<<NAME>>
<<ADDRESS 1>>
<<ADDRESS 2>>
<<CITY, STATE ZIP CODE>>

974 1234 5678 9102 <<Package Code and Membership ID>>

Do not make any address changes to the top half of this authorization form.
Please use the Change of Address Request section below.

Personal Information

OMR
Marks

Signature

I authorize ID TheftSmart to use my personal information to provide credit reports and credit monitoring services to me and to my family members, to the extent permitted by applicable law, and to use my personal information to contact me regarding my credit report and credit monitoring services.

Change of Address Request

Do not complete this section if your address printed above is correct.

Instructions

Step 1. Personal Information

Complete all of the personal information required using black or blue ink only. Please print clearly.

Step 2. Signature

Sign your name and date in the signature box.

Step 3. Verify Printed Address

Please verify that your address printed above is accurate.

If the address above is not your **residential** address, please provide your residential address in the box titled "Change of Address Request."

Step 4. Return Authorization Form

Return this completed form using the postage-paid return envelope we've supplied.

If you do not have your postage-paid return envelope, mail your authorization form to:

Plan Administrator
PO Box 14524
Des Moines, IA 50306-9332

Frequently Asked Questions

Q: What is identity theft?

A: Identity theft is a crime that occurs when someone steals your personal information and uses it to obtain false credit. It often begins with the theft of a Social Security number, credit card number, debit card or phone card.

Q: Where does my identity thief get this information?

Identity thieves can steal information from a variety of places. Several common places where thieves get your contact and bank details for they help themselves to your credit and debit statements, credit card offers and account information, may be your own mailbox or trash can. They may even file a "change of address form" in your name and have all your mail sent to another location. Some thieves fraudulently obtain a credit report in your name. Others take your personal information you share on the Internet.

Q: How do thieves steal the personal information they need?

It's common for an identity thief to call your credit card company and ask for the mailing address on your credit card to be changed. They run up charges on your account and then mail the bills to another address. Other thieves steal your credit card or bank accounts using your name and Social Security Number. Still other thieves steal your checks or the checks bounce back to you in your credit report. Still other thieves steal your name and credit to take out loans for which creditors think you're responsible.

Q: What should I do if I am a victim of identity theft?

As a victim of identity theft, you should make one phone call to the toll-free number shown on the enclosed letter. One of our investigators will contact you and will provide you with all the steps you need to take.

Your ID TheftSmart Benefits

Comprehensive Fraud Restoration

Let the experts do the work for you.

Licensed Investigators who truly understand the problems surrounding identity theft will help restore your name and credit for you. We will do most of the work!

Continuous Credit Monitoring

Early detection is key.

Monitoring your credit is one of the best ways to help spot identity theft early. You can have your credit file continually monitored for specific activity in your Experian credit file. It can alert you to fraud.

If you have questions or feel that you have become a victim of identity theft call the toll-free number shown on the enclosed letter.

Our Licensed Investigators are ready to help you.

Restoration Service Exclusions

Your free Enhanced Identity Theft Restoration service is only available for identity theft concerns that are related to the event described in the cover letter included with this benefits guide.

A signed limited power of attorney must be provided to Kroff when an Identity Theft Restoration case is opened in order for Kroff to work on your behalf and/or provide Non-Credit Database Searches.

Any stolen identity event of which a spouse or child participated in, directed or had prior knowledge.

Any dishonest, criminal, malicious or fraudulent acts, if the member(s) that suffered the fraud personally participated in, directed or had knowledge of such acts.

Membership Services do not cover any financial losses attributed to the Stolen Identity Event, including but not limited to, money stolen from a wallet, unauthorized purchases of retail goods or services online, by phone, mail or direct.

Restoration services only apply to identity theft and fraud issues occurring in the domestic United States.

ID TheftSmart

Your Guide to Membership Benefits



Ways We Guard You Against Identity Theft

Your membership with ID TheftSmart™ gives you easy access to the resources you need to fight back if an identity thief threatens your financial standing. Our services are designed to monitor your credit activity and help restore damage to your credit history.

Enhanced Identity Theft Restoration

Let the experts do the work for you

If you have identity theft or fraud issues related to the event discussed in the cover letter included in this packet, you will have access to Enhanced Identity Theft Restoration to help restore your identity to pre-theft status.

You will also be assigned an experienced Licensed Investigator who will work on your behalf to help resolve your identity theft issues.

Your Licensed Investigator will work on your behalf to help address or correct the identity theft issues you have with affected agencies and institutions, including (but not limited to):

- Credit card companies;
- Financial institutions;
- All three credit repositories;
- Federal Trade Commission;
- Social Security administration;
- Department of Motor Vehicles;
- U.S. Postal Service;
- Law enforcement personnel; and
- other organizations that may be affected.

Your Licensed Investigator will also perform non-credit searches of applicable local and national databases. We'll look for additional issues you may not be aware of, including:

- Criminal activity in your name in your county's records, certain national databases and federal watch lists;
- Department of Motor Vehicle records in your state;
- Unknown addresses affiliated with your Social Security Number; and
- Checking account activity in your name reported as fraudulent.

Continuous Credit Monitoring

Early detection is key

A professional thief can assume your identity in just a few hours. But it can take years for you to restore your credit standing. Early detection is key to minimizing the damage caused by thieves who steal your name.

Continuous Credit Monitoring will alert you to specific activity in your Experian credit file that may be associated with fraudulent activity, such as:

- Companies who have received a copy of your credit report;
- New account information;
- Change of address;
- Public records; and
- Derogatory information.

Upon receipt and review of your monitoring alert, if you feel that you have an identity theft issue, our licensed investigators are available to help restore your name and credit.

Your credit monitoring service cannot be provided without your authorization. You must complete and return the enclosed authorization form to begin the process.



Need assistance? Call the Toll-Free number shown on the enclosed letter.

Privacy Policy

General

Kroll Background America, Inc. ("Kroll") respects your concerns regarding maintaining the privacy of your personal data that is submitted to us. This Privacy Policy covers all the information practices of Kroll and describes the principles Kroll will follow with regard to all information submitted to Kroll in connection with the services we provide. These principles will be implemented by all Kroll personnel regardless of their location. All data shall be collected, stored and used in compliance with the Fair Credit Reporting Act ("FCRA") and other state and federal applicable law. This Privacy Policy applies only to Kroll Background America, Inc. and does not apply to data collected by Kroll Inc. or by any of the subsidiaries of Kroll Inc. other than Kroll Background America, Inc.

Kroll Is Committed to Protecting your Personal Information

Kroll acknowledges both the duty of trust and care in maintaining the privacy of your personal information which we collect and store and our legal obligations as a consumer reporting agency.

- Application Information
- Information From Outside Sources
- Consumer Report Information

Use and Transfer of Information

Kroll is provided with personal information in connection with preparing a report for you. In connection with our providing these services, Kroll may, in some instances, employ other companies and individuals, as our subcontractors, to perform functions on our behalf. All such contractors are contractually obligated to use and maintain the confidentiality of personal information in a manner consistent with this Privacy Policy. These companies may not share any such information with any third party. Except as described in this Privacy Policy, we will not use or otherwise disclose any of the personal data that you provide or that we collect from third parties or other sources.

Confidentiality

Kroll will use our best efforts to insure that no unauthorized parties have access to any of your information. We will never sell or provide your personal data to a third party, except as stated in this Privacy Policy, without your express consent. We may, however, disclose personal data in response to a court order or other legal obligation.

Accuracy

Kroll makes every effort to ensure that the data we receive, collect, and store about you is as accurate as possible. However, Kroll does not vouch for, and is not responsible for, incomplete, inaccurate or not current data about you that may be supplied to Kroll by a third-party source.

Access

You have the right to access any reports Kroll produces and maintains about you. You may contact Kroll at any time to determine whether we hold any personal information about you and to obtain access to that information. We will only afford you access to your data upon proof of identification that you are the individual who is entitled to request access. We will mail a copy of such information within 7 days as mandated by the FCRA.

Security

Protecting your confidential information is our business; therefore, Kroll takes all appropriate measures to assure the security of your personal data. Kroll uses advanced encryption technology – 128-bit Secure Socket Layer (SSL) - to keep personal information and data secure from unauthorized access. All data is stored on our servers in a secure, encrypted manner. Access to those servers is strictly limited to network administrators and other authorized personnel of Kroll, who have been trained to protect against loss, misuse, unauthorized access, disclosure, alteration or destruction of personal data under Kroll's control. We take pride in our technology and our security policies.

Kroll is a member of the Better Business Bureau and the Better Business Bureau Online Privacy Seal Program. The Better Business Bureau is available for resolving disputes between you and Kroll. To file a complaint with respect to the privacy practices of Kroll, you may visit the Better Business Bureau web site at www.bbbonline.com

KROLL

Know Your Rights

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment — or to take another adverse action against you — must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, as of September 2005 all consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.ftc.gov/credit for additional information.

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. See www.ftc.gov/credit for an explanation of dispute procedures.

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need — usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.ftc.gov/credit.

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit.

Para informacion en espanol, visite www.ftc.gov/credit o escriba a la FTC Consumer Response Center, Room 130-A, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580

States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General. Federal enforcers are:

Type of Business:	Contact:
Consumer reporting agencies, creditors and others not listed below	Federal Trade Commission: Consumer Response Center – FCRA, Washington, DC 20580 877-382-4357
National banks, federal branches/agencies of foreign banks (word "National" or initials "N.A." appear in or after bank's name)	Office of the Comptroller of the Currency, Compliance Management, Mail Stop 6-6, Washington, DC 20219 800-613-6743
Federal Reserve System member banks (except national banks, and federal branches/agencies of foreign banks)	Federal Reserve Board, Division of Consumer & Community Affairs, Washington, DC 20551 202-452-3693
Savings associations and federally chartered savings banks (word "Federal" or initials "F.S.B." appear in federal institution's name)	Office of Thrift Supervision, Consumer Complaints, Washington, DC 20552 800-842-6929
Federal credit unions (words "Federal Credit Union" appear in institution's name)	National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314 703-519-4600
State-chartered banks that are not members of the Federal Reserve System	Federal Deposit Insurance Corporation, Consumer Response Center, 2345 Grand Avenue, Suite 100, Kansas City, Missouri 64108-2638 877-275-3342
Air, surface, or rail common carriers regulated by former Civil Aeronautics Board or Interstate Commerce Commission	Department of Transportation, Office of Financial Management, Washington, DC 20590 202-366-1306
Activities subject to the Packers and Stockyards Act of 1921	Department of Agriculture, Office of Deputy Administrator – GIPSA, Washington, DC 20250 202-720-7051

NO POSTAGE
NECESSARY
IF MAILED
IN THE UNITED
STATES



BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 935B DES MOINES IA

POSTAGE WILL BE PAID BY ADDRESSEE

ADMINISTRATOR
PO Box 14524
DES MOINES IA 50306-9332



7501 123 4-0706

Pikowski Richard

From: Pikowski Richard
Sent: Tuesday, March 25, 2008 6:27 PM
Subject: Important Notice-Action Required

Importance: High

Dear Colleague,

I wish to bring the following security issue to your attention.

One of our third party vendors, USInternetworking Inc. ("USI") informed us today that a laptop was recently stolen from the home one of their employees.

I am advised that 2 of the files on the laptop contained personal information (name, address and social security number) of some XL employees.

USI have advised that the laptop was password protected and there is no evidence that XL employees' personal information has been, or will be, used for unauthorized purposes. However, as a precaution, I am notifying you that the possibility exists that this information could be used to open or access your credit accounts..

XL is working with USI to do everything possible to address this issue.

Meanwhile, it is recommended that you notify any financial institutions where you may have accounts such as banks, credit card companies, and brokerage firms to alert them of the breach.

I will provide an update on this situation as soon as possible.

Fraud Alerts

It is recommended that you 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

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

Richard Pikowski
Senior Vice President
Head of Global HR Operations
XL Global Services Inc.
Seaview House
70 Seaview Avenue
Stamford, Ct. 06902, USA
Phone +1 203-964-5239
Fax +1 203-964-9811
richard.pikowski@xlgroup.com
www.xlcapital.com

Pikowski Richard

From: Pikowski Richard
Sent: Thursday, March 27, 2008 9:37 AM
Subject: Update-RE: Important Notice-Action Required

Importance: High

We've been actively working with our partner to acquire additional information and to discuss credit protection services through a third party that would include credit restoration services (if needed) to be provided to each of you at no cost. This is a very fluid situation and we recognize this is causing a high degree of concern and frustration for all. We hope to have a thorough Q&A and a description of the services to you as soon as possible. Thank you for your patience.

Richard Pikowski
Senior Vice President
Head of Global HR Operations
XL Global Services Inc.
Seaview House
70 Seaview Avenue
Stamford, Ct. 06902, USA
Phone +1 203-964-5239
Fax +1 203-964-9811
richard.pikowski@xlgroup.com
www.xlcapital.com

Pikowski Richard

From: Pikowski Richard
Sent: Friday, March 28, 2008 9:58 AM
Subject: Further Update: RE: Important Notice-Action Required

Importance: High

Attachments: FAQs_USI-FINAL.doc

As initially reported to you via email on March 25th, XL was informed by one of its third party vendors, USInternetworking Inc. ("USi"), of the theft of a laptop computer containing personal identifying information, including names, addresses and social security numbers.

On behalf of USi and XL, we deeply regret this incident and want you to know that we are committed to working together to enhance the protection of your personal identifying information to avoid inappropriate disclosures in the future.

As a result, USi and XL are pleased to offer to each affected employee - free of charge - two years of credit monitoring and identity theft protection and, if necessary, credit recovery services through Kroll, Incorporated ("Kroll"). Kroll is a leading provider of risk consulting services, providing a broad range of investigative, intelligence, financial, security and technology services. Kroll's Fraud Solution practice provides credit monitoring, identity theft protection and credit recovery services. Next week, you will receive a packet of information from Kroll outlining "ID TheftSmart" one of the most comprehensive programs available to protect you against identity theft. Please note that in order to activate the services, you will need to complete and submit the form in order to ensure your enrollment in the "ID TheftSmart" program.

To date, we have no evidence that your personal identifying information has been, or will be, used for unauthorized purposes; however, as we indicated in its earlier emails, prudent safeguards of your credit ratings and accounts are advised.

We sincerely hope that you find the services offered by Kroll a worthwhile solution.

We have also provided some more details and information in the attached Q&As. Please note that these Q&As will be updated as and when new information is received. We hope that you will find them useful. Lastly, please note that if you are receiving this email that you were affected by the incident.

Sincerely,
Richard Pikowski



FAQs_USI-FINAL.doc
c (57 KB)

Richard Pikowski
Senior Vice President
Head of Global HR Operations
XL Global Services Inc.
Seaview House
70 Seaview Avenue
Stamford, Ct. 06902, USA

The following questions are compiled from the various questions received to date. The document will be updated as and when new info is received

Questions about the incident

What happened which has led to certain XL employees' personal data potentially being compromised or susceptible to identity theft?

The home of USinternetworking Inc. ("USi") employee was burgled on Sunday, March 23, 2008. USi, a third party vendor of XL's, informed us on Tuesday, March 25, 2008 of the burglary and advised that amongst the items stolen from the home was a work laptop which included two files holding personal information of some XL employees.

What personal information was contained on the laptop?

USi has informed us that the two files on the laptop, which was password protected, held XL data. One file had NAME and SS# only and the other had NAME, ADDRESS and SS#.

Was a police report filed?

Yes. USi advised that a police report was filed with the local police where the incident took place. At this time, no copies of the police report are being provided in part because law enforcement at this time are concerned that the investigation could be compromised if the report is broadly released.

What information is being provided by the police?

The Police have advised USi that the release of report at this time can jeopardize the investigation. In most of these cases, the laptop is stolen by some thief who will 'wipe' or 'clear' the hard-drive and sell the laptop for a few hundred dollars. However, if exact details of the crime are publicized, we may be alerting the thief to the fact that the data on the computer is much more valuable than the computer itself. We understand that the police have interviewed a number of people in the area as well as checked local pawn shops, flea markets and other areas where stolen items are often surfaced for resale.

What are the implications of such personal information being stolen?

It is our understanding that in addition to the individual's work laptop, other household goods were also stolen. At this time, there is no indication that the thieves are aware of what data is held on the laptop and the assumption is that the thief could wipe the hard drive clean and sell it as a second hand laptop.

We can only speculate as to what a potential fraudster may do with the data held on the laptop. Based on what we have seen in the media and advice received, it appears that the data can be used to create new accounts and false identification cards that could then be used to access your personal accounts.

What other additional information do you have about the theft or the investigation?

We have no further information at this time, but will certainly provide further updates as and when we receive them.

Questions about USi and their response to the incident

Who is USinternetworking?

USinternetworking, Inc. (USi), an AT&T company, is an Application Service Provider (ASP). They use a highly automated, efficient, systematic approach to deliver managed hosting, application management, remote management, professional services, SaaS enablement and eBusiness development and hosting

services to more than 150 enterprise-level organizations in over 30 countries. More information about USi can be found at <http://www.usi.com>

What services does USi provide XL?

XL has outsourced application, software, and hardware/infrastructure support services for its PeopleSoft HR, PeopleSoft Financials, and Business Objects Planning systems, including disaster recovery environments, to USi. As demand dictates, we also contract with USi for professional services to develop, test, and implement new or changed functionality in our HR system. XL ensures that USi undergoes audits and examinations to validate processes and controls against industry-defined standards and government regulations.

Why did USi have certain XL employees' personal information on a laptop at one of their employee's homes?

The data was made available in this instance in order to test and implement certain changed functionality within the HR systems. However, the files were inappropriately residing on this individual's laptop. We have since been assured that the appropriate steps have been taken by USi to address this breach as well as measures to ensure that this does not happen again.

The nature of USi's business requires them to undergo various audits and examinations to validate their processes and controls against industry-defined standards, government regulations, and their own internal standards as well as that of XL's IT Security team. More information on USi's audits, examinations and certifications can be found at <http://www.usi.com/compliance-program.aspx>

How is it that only certain employees' names and information were provided to USi?

As a general rule, whenever XL implements, enhances or alters a program, it is subject to a series of tests in order to review the impact it will have on existing applications and to correct any issues before it goes into live production. One of the last tests that are run before going live utilizes a random selection of live data that is run through the gamut of tests in an environment that mirrors the live system.

How is USi assisting affected XL employees as a result of this incident?

USi reported the issue to authorities and also sent their own security team to the location to assist the local authorities who are handling the investigation. USi has also assured us that they have taken the appropriate steps to address this breach as well as measures to ensure that this does not happen again.

Furthermore, USi has engaged Kroll, Incorporated ("Kroll"), to provide the necessary services to further protect you and your information. Kroll is a leading provider of risk consulting services, providing a broad range of investigative, intelligence, financial, security and technology services. Kroll's Fraud Solution practice provides credit monitoring, identity theft protection and credit recovery services.

For more than 30 years, Kroll has helped companies, government agencies and individuals reduce their exposure to risk and capitalize on business opportunities. Kroll is an operating unit of Marsh & McLennan Companies, Inc., the global professional services firm. More information about Kroll can be found at www.kroll.com.

How will Kroll's services help those XL employees who may be potentially affected by identity theft, fraud etc.?

Kroll Inc., the world's leading risk consulting company, is providing you with access to its ID TheftSmart™ Enhanced Identity Theft Restoration and Continuous Credit Monitoring, all at no cost to you. ID TheftSmart is one of the most comprehensive programs available to help protect against identity theft.

How do I contact Kroll to begin using their services?

We urge you to take the time to read about the safeguards that will be included in the enrollment package that will be sent to you within the next week. The package will include your membership number, plastic membership card as well as the toll free number(s) needed in order to access the ID TheftSmart member services.

How long will I have access to the Kroll services?

You will have access to the Kroll services for 24 months (12 months longer than the standard package). However, should you require credit recovery support as a result of this breach, that service will continue for as long as necessary.

Questions about employees' personal matters related to the incident

Will I have to monitor my credit reports as a result of this incident?

Yes, you will have to monitor your credit reports and act upon any suspicious activity. Again, in order to assist you with this process, USi has engaged Kroll, Incorporated ("Kroll"). Kroll's Fraud Solution practice provides credit monitoring, identity theft protection and credit recovery services as detailed in the attached packet of information

How difficult will it be dealing with credit agencies once I issue my fraud alert?

We recognize the impact that this may have on you. However, the services provided by Kroll is equipped to assist you with this process.

Do I need to freeze my existing bank accounts and reopen new ones?

While we are not advising employees to freeze their existing accounts and reopen new ones, we understand that some financial institutions are requiring it, while others have other methods for protecting your accounts (e.g. through the use of a unique password). We urge employees to heed the directions of their providers and encourage you to take reasonable steps that you feel are necessary in order to protect your identify.

Please remember to communicate any account changes to the Payroll Department so that your next paycheck can be appropriately routed.

Who at XL is handling the matter?

As soon as XL became aware of the incident, we pulled together a team comprised as follows:

- Richard Pikowski, Global HR Operations
- Cynthia Dubs, IT Team Leader
- Thomas Dunbar, Global IT Chief Security Officer
- Jo-Anne Steele, HR Global Systems Manager
- Danielle Barone, HR Regional Operations Manager – Americas,
- Daniel Losito, Associate General Counsel - Global Labor and Employment Law
- Norma A Nielsen, Associate General Counsel and Chief Privacy Officer
- Carolyn Moss, Corporate Communications

Who do I contact if I have more questions?

If you have questions or feel you may have become a victim of identity theft, please call ID TheftSmart member services on either the national or international toll free numbers provided in enrollment pack.

For general questions, please contact Richard Pikowski, Global HR Operations.

Pikowski Richard

From: Pikowski Richard
Sent: Friday, April 04, 2008 5:40 PM
Subject: Update on mailing of packets from Kroll: RE: Important Notice-Action Required

Dear Colleagues,

Further to my email below, I regret to inform you that USInternetworking ("USi") has experienced a delay in distributing Kroll's "ID TheftSmart" information packs to you.

We would like to express our sincere apologies for this delay which we understand would only add to your anxiety in this matter. USi have informed us that they are working diligently to get this information out to you early next week and will be sending the packages via USPS Next Day service. We will of course keep you updated on this situation and will notify you as soon as we know the packages have been mailed.

On behalf of XL, I would like to stress that we are working very hard to make this crucial information pertaining to Kroll's services available to you. We are extremely disappointed by this news from USi, but remain committed to working with them to address this matter and to enhance the protection of your personal identifying information to avoid inappropriate disclosures in the future.

To date, we still have no evidence that your personal identifying information has been, or will be, used for unauthorized purposes; however, as we have stated before, prudent safeguards of your credit ratings and accounts are advised.

Should you have any questions or concerns between now and our next update, please feel free to contact me.

From: Pikowski Richard
Sent: Friday, March 28, 2008 9:58 AM
Subject: Further Update: RE: Important Notice-Action Required
Importance: High

As initially reported to you via email on March 25th, XL was informed by one of its third party vendors, USInternetworking Inc. ("USi"), of the theft of a laptop computer containing personal identifying information, including names, addresses and social security numbers.

On behalf of USi and XL, we deeply regret this incident and want you to know that we are committed to working together to enhance the protection of your personal identifying information to avoid inappropriate disclosures in the future.

As a result, USi and XL are pleased to offer to each affected employee - free of charge - two years of credit monitoring and identity theft protection and, if necessary, credit recovery services through Kroll, Incorporated ("Kroll"). Kroll is a leading provider of risk consulting services, providing a broad range of investigative, intelligence, financial, security and technology services. Kroll's Fraud Solution practice provides credit monitoring, identity theft protection and credit recovery services. Next week, you will receive a packet of information from Kroll outlining "ID TheftSmart" one of the most comprehensive programs available to protect you against identity theft. Please note that in order to activate the services, you will need to complete and submit the form in order to ensure your enrollment in the "ID TheftSmart" program.

To date, we have no evidence that your personal identifying information has been, or will be, used for unauthorized purposes; however, as we indicated in its earlier emails, prudent safeguards of your credit ratings and accounts are advised.

We sincerely hope that you find the services offered by Kroll a worthwhile solution.

We have also provided some more details and information in the attached Q&As. Please note that these Q&As will be updated as and when new information is received. We hope that you will find them useful. Lastly, please note that if you are receiving this email that you were affected by the incident.

Sincerely,
Richard Pikowski

Richard Pikowski
Senior Vice President
Head of Global HR Operations
XL Global Services Inc.
Seaview House
70 Seaview Avenue
Stamford, Ct. 06902, USA
Phone +1 203-964-5239
Fax +1 203-964-9811
richard.pikowski@xlgroup.com
www.xlcapital.com

Pikowski Richard

From: Pikowski Richard
Sent: Wednesday, April 09, 2008 11:29 AM
Subject: Details on the mailing of packets from Kroll: RE: Important Notice-Action Required

Importance: High

I am pleased to confirm that Kroll's "ID TheftSmart" information packs were mailed today to your home addresses via USPS Priority service. You should expect to receive the information no later than Friday. If you experience any delays, please contact me.

Upon receiving your information packs, please note that you will need to complete and mail the enrollment form to Kroll in order to activate "ID TheftSmart" services. We strongly advise that you do register for "ID TheftSmart", one of the most comprehensive programs available to protect you against identity theft.

If you have any questions or concerns once you have received your information, please refer to the Kroll Member Services telephone number included in the pack. "ID TheftSmart" will be provided free of charge for two years, which includes credit monitoring, identity theft protection and, if necessary, credit recovery services.

At any time during this two-year period should you become the unfortunate victim of a theft/fraud, please kindly notify me or your local HR Generalist. XL would like to be kept informed of any matters potentially related to this incident, however, Kroll does not have any obligation to inform XL should one be reported.

On behalf of XL, I would like to reiterate again how deeply we regret that this incident occurred. XL is reviewing and addressing this situation so that we can avoid inappropriate disclosures in the future.

Richard Pikowski
Senior Vice President
Head of Global HR Operations
XL Global Services Inc.
Seaview House
70 Seaview Avenue
Stamford, Ct. 06902, USA
Phone +1 203-964-5239
Fax +1 203-964-9811
richard.pikowski@xlgroup.com
www.xlcapital.com