

**North Carolina Security Breach Reporting Form  
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: Ryerson Inc.

Address: 2621 W. 15<sup>th</sup> Place  
Chicago, IL 60608

Telephone: (773) 788-3356

Fax: (773) 762-2194

Email: Andrew.Bruns@ryerson.com

**PLEASE SUBMIT FORM TO:**

Consumer Protection Division  
NC Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
Telephone: (919) 716-6000  
Toll Free I NC: (877) 566-7226  
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: April 16, 2008

Date the Security Breach was discovered: April 3, 2008

Estimated number of affected individuals: 410

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. §75-65(b)): Ernst & Young, LLP

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: A laptop was stolen from an Ernst & Young accountant and Ernst & Young has now informed Ryerson that said laptop may have contained an electronic file with the names and social security numbers of some current and former Ryerson employees.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner: Yes. If so, please describe the security measures protecting the information: Ernst & Young has informed Ryerson that "Subject data was encrypted with multiple security passwords."

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Ernst & Young reports that "... it will continue to train end-users to ensure that all security measures in place are complied with."

Date affected NC residents were/will be notified: April 16, 2008

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. §75-65(a) and (c): The laptop was stolen from an Ernst & Young accountant on January 3, 2008. On April 3, 2008, Ernst & Young completed the data base review and informed Ryerson of the confidential Ryerson employee information that may have been on the laptop stolen from them.

If the delay was pursuant to a request from law enforcement pursuant to N.C. G.S. 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?

(pursuant to N.C.G.S. § 75-65(e))

Please attach a copy of the notice if in written form or a copy of Any scripted notice if in telephonic form.

- written notice
- electronic notice (email)
- telephone notice
- substitute notice

Signature:  Date: April 16, 2008

Contact Person, Title: Andrew M. Bruns, Vice President, Human Resources

Address: \_\_\_\_\_

(if different from above)

Telephone: (773) 788-3356 Fax: (773) 762-2194 Email: Andrew.Bruns@ryerson.com



2821 West 15<sup>th</sup> Place  
Chicago, IL 60609

April 16, 2008

«Fname» «Lname»  
«Address Street Line 1»  
«City», «State» «Zip»

Dear «Fname»:

As part of our company's regular processes to verify our financial records, Ryerson has used a leading professional services provider, Ernst & Young, LLP to perform external auditing of our records. As part of the process, Ernst & Young is occasionally provided with some employee information to verify the accuracy of the financial records.

I am writing to let you know that there was a recent theft of a briefcase containing a laptop computer from the car of an Ernst & Young accountant. Ernst & Young has reviewed the backup files from the computer and believes that your name and social security number may have been included in one of the files on the stolen laptop.

Ryerson takes the security of our employees' personal information very seriously, and we deeply regret that this incident incurred. Ernst & Young has assured Ryerson that the data on the stolen laptop was protected by encryption, as well as other various security measures. We have no reason to believe that any of the data on the stolen laptop has been misused, or even accessed. However, because we are not able to rule out this possibility entirely, you may wish to consider taking steps to protect your personal information.

At our request, Ernst & Young has established a toll-free help line at 888-659-8725 to assist you with questions and concerns you may have or if you believe you have been a recent victim of identity theft related to this incident. The help line will be staffed from 8:00 a.m. to 7:00 p.m. central time, Monday through Friday, from now until May 16, 2008. If you need to call after hours, you may leave a message, and we have been assured you will receive a call back on the next business day.

We have arranged for you, at your option, to enroll in credit monitoring, at no cost to you, for the next year. Once you enroll, you will receive communications detailing any changes to your credit reports from all three credit bureaus. To enroll in this service, please visit <http://partner.consumerinfo.com/ey> and enter the code provided below. You will be instructed on how to initiate your online membership. If you do not have internet access, please contact the toll-free help line described above.

Website for enrollment: <http://partner.consumerinfo.com/ey>  
Your promotional code: «Code»

«Fname» «Lname»

Page Two

April 16, 2008

In addition, upon a request from you, the three major U.S. credit bureaus will place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. There is no charge for this service. However, because it tells creditors to follow certain procedures to protect you, it may delay your ability to obtain credit in some instances. You may initiate a fraud alert for all three major bureaus by contacting any one of them at the following numbers or websites:

<u>Agency</u>	<u>Toll Free Number</u>	<u>Website Address</u>
Experian	(888) 397-3742	<a href="http://www.experian.com">www.experian.com</a>
Equifax	(800) 525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
TransUnion	(800) 680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

The company you contact is required to contact the other two credit bureaus, which will place an alert on their versions of your report as well. You are entitled to order one free credit report from each of the three nationwide consumer reporting companies, and if you ask, only the last four digits of your Social Security number will appear on your credit reports. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228. For your reference, we have enclosed an informational document that addresses a number of frequently asked questions. For additional information on how to further protect yourself against identity theft, you may wish to visit the Website of the U.S. Federal Trade Commission at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

If we become aware of any instance in which the information on the stolen laptop may have been accessed or misused, we will alert you immediately of additional steps that can and should be taken.

Again, we deeply regret any inconvenience or concern this incident may cause you. Be assured that we are committed to continuing to take whatever steps are appropriate to protect confidential employee information.

Sincerely,



Andrew M. Bruns  
 Vice President, Human Resources  
 Ryerson Inc.

Enc.

**Frequently Asked Questions  
April 2008  
Data Security Incident**

**What happened and how does this affect me?**

A laptop was stolen from the external vendor (Ernst & Young LLP) with whom Ryerson contracts to audit our financial statements for accuracy. The laptop had an electronic data file stored on it which included identifying information for some former and current Ryerson employees. The data lost included the name and social security number of some employees and former employees. All former and current employees who may have been affected have been notified regarding this issue.

The authorities believe the computer equipment, rather than any of the data on it, was the target of the theft.

**Why did this company have my name and social security number on the computer?**

Ryerson contracts with Ernst & Young, LLP to provide external auditing of financial records. As part of the ongoing process, Ernst & Young is provided with some employee information, including name and social security number, in order to allow them to verify the accuracy of the financial records.

**Is it a common practice to allow data of this nature to be accessed by private contractors?**

Ryerson, like most companies, contracts with external auditing companies to have the financial statements checked for accuracy by an independent third party. We are working with our external auditing companies to ensure our employees' and former employees' data receives the highest standard of security and privacy protection.

**What should I do to protect myself? Do I have to close my bank account or cancel my credit cards?**

At this point in time, we have no confirmation of misuse of Ryerson employee and former employee data resulting from the laptop theft from an Ernst and Young LLP accountant. Because name and Social Security Numbers were contained in a file on this computer, we advise individuals to monitor financial accounts continuously for suspicious activity as a matter of good practice. For tips on how to guard against misuse of personal information, visit the Federal Trade Commission website at <http://www.ftc.gov/>.

You do not have to close your bank account or cancel your credit cards. You should however take steps to protect yourself against identity theft. We advise you to monitor your financial accounts continuously for suspicious activity. One way to monitor your financial reports is to review your credit report. By law you are entitled to one free credit report each year from each of the 3 major credit bureaus. You can request a free credit report from one of the three major credit bureaus – Equifax, Experian, or TransUnion – at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling 1-877-322-8228

**What do you mean by suspicious activity?**

Suspicious activity could include the following:

- Inquiries from companies you have not contacted or done business with;
- Purchases or charges on your accounts that you did not make;
- Calls or letters about purchases you did not make;
- New accounts you did not open or changes to existing accounts you did not make;
- Bills that do not arrive as expected;
- Unexpected credit cards or account statements; or
- Denials of credit for no apparent reason.

**I do not detect any suspicious activity, but am concerned about this issue, what else can I do?**

You may want to take the precaution of placing a fraud alert on your credit files.

**What is a fraud alert?**

There are 2 types of fraud alerts: an **initial alert** and an **extended alert**.

An **initial alert** stays on your credit report for at least 90 days. By placing the initial alert on your credit report, potential creditors must use what the law refers to as "reasonable policies and procedures" to verify your identity before

**Frequently Asked Questions  
April 2008  
Data Security Incident**

issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you. When you place an initial fraud alert on your credit report, you are entitled to one free credit report from each of the 3 nationwide consumer reporting companies, and if you ask, only the last four digits of your Social Security number will appear on your credit reports.

An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you have been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. With an extended fraud alert, potential creditors must actually contact you, or meet with you in person, before they issue you credit. When you place an extended alert on your credit report, you are entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

To place either type of fraud alert on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity. This may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

Placing either type of fraud alert on your credit report may cause some delays if you are trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

**What does a fraud alert not do?**

While a fraud alert can help keep an identity thief from opening new accounts in your name, it is not a solution to all types of identity theft. It will not protect you from an identity thief using your existing credit cards or other accounts. It also will not protect you from an identity thief opening new accounts in your name that do not require a credit check – such as a telephone, wireless, or bank account. If there is identity theft already going on when you place the fraud alert, the fraud alert alone will not stop it. A fraud alert, however, can be extremely useful in stopping identity theft that involves opening a new line of credit.

**Can the Social Security Administration put a flag on my Social Security number?**

No, unlike the credit bureaus, the Social Security Administration (SSA) cannot put a flag or security alert of any type on your Social Security number.

To report that someone is using your Social Security number, file a complaint with the Federal Trade Commission following the process listed above.

**Should I apply for a new Social Security number?**

Under certain circumstances, the Social Security Administration may issue you a new Social Security number – at your request – if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new Social Security number may not resolve your identity theft problems, and may actually create new problems. For example, a new Social Security number does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with those from your new Social Security number. Even when the old credit information is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult for you to get credit. Finally, there is no guarantee that a new Social Security number would not also be misused by an identity thief.

**What are my remedies if my identity is stolen and used illegally?**

The Federal Trade Commission has produced a booklet to help you remedy the effects of an identity theft. It describes what steps to take, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future. The contents of the booklet, *Taking Charge: Fighting Back Against Identity Theft*, are available online at <http://www.usaa.gov/veteransinfo.shtml>.