



THOMSON REUTERS

Jeff Rohlmeier
Director of Privacy & Compliance

610 Opperman Drive
Eagan, MN 55123

D 651-848-5550
jeff.rohlmeier@thomsonreuters.com

February 23, 2010

Via Registered Mail

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Notification of Possible Thomson CompuMark Data Security Breach

Dear Sir(s):

I am writing to report a data security breach that requires notification under Maryland law. This letter explains the incident and summarizes the ways we are protecting the affected individuals from possible harm. A copy of the letter to be sent to affected individuals is also enclosed.

On January 21, 2010, the St. Paul, Minnesota Police Department contacted us regarding an investigation of a residential burglary involving one of our employees. During the course of their investigation, the police collected information suggesting that the employee may have inappropriately removed certain paperwork with Thomson CompuMark customer payment card information from our offices. The information may have included the customers' names, addresses and payment card numbers. Between May and December of 2009, the employee processed payments received from approximately 140 Thomson CompuMark customers, including three residents of Maryland. The employee processed only manual payments and did not have access to information in our electronic payment systems. Upon learning of the unauthorized removal of sensitive information, we terminated the employee. To date, we have not received any reports from our customers that they have been subject to any unauthorized activity relating to this incident. However, we are taking certain steps to enable our customers to mitigate certain risks associated with this incident. As you can see, we have contracted with Experian® so that the individuals receive free daily credit monitoring of all three national consumer reporting agency files as well as fraud resolution services and identity theft insurance. We have also set up a telephone line to answer any questions that these individuals may have. Moreover, we have initiated steps to bolster our own physical, administrative and technical safeguards around certain sensitive customer information to mitigate the risk of recurrence.



THOMSON REUTERS

Maryland Office of the Attorney General
February 23, 2010
Page 2

We deeply regret this incident. Please let me know if your office has any questions.

Sincerely,

Jeff Rohlmeier
Director of Privacy & Compliance
Thomson Reuters – Legal

Enclosure

March 1, 2010

[Mailing Address of Data

Subject/Customer to be

Notified]

RE: Notification of Possible Thomson CompuMark Data Security Breach

Dear Mr./Ms. XXXXXX:

I am writing to inform you that Thomson CompuMark has experienced an incident that may have exposed your personal information, including your credit card number ending in XXXX. We deeply regret this incident. This letter explains what happened and what steps we are taking to minimize any risks that you may face as a result.

What Happened?

On January 21, 2010, the St. Paul, Minnesota Police Department contacted us regarding an investigation of a residential burglary involving one of our employees. During the course of the investigation, the police collected information suggesting that the employee in question may have inappropriately removed certain paperwork containing customer credit card information from our offices. The information may have included your name, address and credit card number. Between May and December of 2009, the employee processed credit card payments received from approximately 140 Thomson CompuMark customers, including yours. The employee processed only manual payments and did not have access to information in our electronic payment systems. Upon learning of the unauthorized removal of sensitive information, we terminated the employee. Though this incident appears to be a crime of opportunity, we are also reviewing our own physical, administrative and technical safeguards around sensitive customer information to minimize the risk of recurrence.

What are the Risks that Your Information Will be Misused?

To date, we have not received any reports from our customers that they have been subject to any unauthorized activity as a result of this incident. Nevertheless, you should consider contacting your credit card company and request a replacement card. You should also closely inspect your past credit card statements for any unauthorized transactions. Since credit card fraud trends are often difficult to predict, you should also remain vigilant against any future unusual activities. Our investigation and that of the police department continues.

How Can You Protect Yourself?

We recommend that you be vigilant to any signs of fraud or identity theft. You should also understand that you can take certain steps to obtain further information and to protect yourself from identity theft.

Thomson CompuMark has partnered with ConsumerInfo.com, an Experian® company, to provide you with a full year of free credit monitoring. This credit monitoring product, Triple Advantage^(SM), notifies you of key changes to all three of your national credit reports that could be signs of identity theft. It will help you to identify any possible fraudulent use of your information.

We strongly recommend that you participate in this program. Once you enroll, your *complimentary 12-month membership includes:*

- A free copy of your Experian, Equifax and TransUnion credit reports
- Daily monitoring and timely alerts of any key changes to your credit reports—so you know when there is any activity that you should be made aware of such as notification of new inquiries, newly opened accounts, delinquencies, public records or address changes
- Unlimited, on-demand access to your Experian credit report and PlusScoreSM for the duration of your membership.
- Access to a dedicated team of fraud resolution representatives who will help you investigate each incident; contact credit grantors to dispute charges, close accounts if necessary, and compile documents; and contact all relevant government agencies.
- \$25,000 in identity theft insurance coverage (\$10,000 for New York state residents) with zero deductible provided by Virginia Surety Company, Inc. for certain identity theft expenses

You have ninety (90) days to activate this membership, which will then continue for a full year. We encourage you to activate your credit monitoring membership quickly.

- **To sign up online**, please visit <http://partner.consumerinfo.com/premium> and enter your individual Credit Monitoring Access Code provided below. Please keep in mind that once activated the code cannot be re-used. You will be instructed on how to enroll in your complimentary credit monitoring product. If you sign up online, all credit reports and alerts will be delivered via email.
- **To sign up by telephone**, dial +1-866-252-0121.

Your Single Use Credit Monitoring Access Code: <<Code>>

Should You Do Anything Else?

Whether or not you choose not to enroll in the credit monitoring service, we recommend that you carefully monitor all of your credit [debit] card statements, other account statements and your credit reports to make certain there have been no unauthorized transactions made or new accounts opened in your name. Contact your financial institution immediately if there is any unauthorized activity on your accounts or if an unauthorized account has been opened in your name.

Credit Reports. You may obtain a free copy of your credit report once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free +1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the request form at <http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm>). (Please note that you receive your credit reports from the three national credit report companies when you sign up for the Triple Advantage product.) You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies.

Fraud Alert. Further, you may wish to contact one of the three major credit bureaus to request that an initial free 90-day fraud alert be added to your file (the other two credit bureaus will be notified automatically). Fraud alerts notify potential creditors to verify the identity of anyone seeking credit in your name before they extend credit in case someone is using your information without your consent. Contact information for each of the three credit bureaus is listed below:

Equifax	Experian	TransUnion
+1-800-525-6285	+1-888-397-3742	+1-800-680-7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance
Atlanta, GA 30374-0241	Allen, TX 75013	Department
http://www.equifax.com	http://www.experian.com	P.O. Box 6790
		Fullerton, CA 92834-6790
		http://www.transunion.com

Where Can You Go for More Information?

Further guidance on how to protect yourself against identify theft is also available from the FTC at the FTC Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580; Phone: +1-877-IDTHEFT (438-4338), Website: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>. You may also contact the Maryland Attorney General's Office at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Phone: +1(888) 743-0023; Website: www.oag.state.md.us, for further information regarding steps that you can take to protect yourself against identity theft.

If you want to learn more about identify theft, you may wish to visit The Identity Theft Resource Center, a non-profit organization that you can contact online at <http://www.idtheftcenter.org/> or via e-mail at itrc@idtheftcenter.org.

Thomson CompuMark extends its sincerest apologies for this event. If you should have any additional questions or concerns about this incident, please do not hesitate to reach me at PH: +1-617-376-7778, or anne.olson@thomsonreuters.com.

Sincerely,

[SIGNATURE]

Anne Olson

Vice President for Research & Content Services

Thomson Reuters – Legal