IHS Jane's Payment Card Data Population – U.S.

[Insert date]

[Name]
[Address]
[City], [State] [ZIP]

Dear **[Name]**,

We are writing to notify you of a data security incident involving IHS Inc. On February 22, 2013, IHS discovered that some of our databases, including those containing personal information you provided as a customer of IHS Jane's, were illegally accessed by unauthorized parties. Our investigation indicates that the unauthorized parties acquired the relevant data from the IHS Jane's environment on or about November 22, 2012.

IHS worked with law enforcement authorities to investigate this cyber attack. In addition, we had retained experts in data security to conduct a forensic investigation. Based on the investigation, the relevant information accessed by the unauthorized parties includes some customer names, contact information, user names, passwords, payment card numbers and expiration dates. Our investigation indicates that most of the affected payment cards have already expired and was part of the historical records in the Jane's legacy databases. We have taken significant steps to prevent this type of incident from reoccurring, which included securing of our systems and enhancing our data security safeguards.

We regret that this incident affects you. We take our obligation to safeguard your personal information very seriously and we are alerting you so you can take steps to protect yourself. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you detect any fraudulent charges on your payment card account, we recommend that you immediately contact your bank or payment card company, and local law enforcement authorities. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. The attached Reference Guide provides details on these and other steps you may wish to consider, including recommendations by the U.S. Federal Trade Commission on the protection of your personal information. You also may want to place a fraud alert or security freeze on your credit file.

For your protection, we have automatically reset individual passwords. If your password was affected, you should have received information by email from us about how to retrieve your new password. We also recommend that users with impacted passwords change their passwords on any other website on which they use a password that is the same as or similar to their IHS Jane's account password.

We hope this information is useful to you. If you have any questions regarding this incident, please call the IHS Care Team at: +1 800 IHS-Care (+1 800 447-2273), Monday through Friday 08:00 to 18:00pm [MT].

Again, we deeply regret any inconvenience this may cause you.

Sincerely,

Scott Key
President and COO
IHS Inc.

Reference Guide

We encourage individuals receiving IHS' letter to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	1-800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 6790 Fullerton, California 92834-6790	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit bureaus without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually*. For more information on security freezes, you may contact the three nationwide credit bureaus or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three nationwide credit bureaus to find out more information.

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. The credit bureaus may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report. You have the right to obtain a police report if you are the victim of identity theft. **For North Carolina Residents.** You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Mail Service Center 9001
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov