EDWARDS WILDMAN

EDWARDS WILDMAN PALMER LLP
20 CHURCH STREET
HARTFORD, CT 06103
+1 860 525 5065 main +1 860 527 4198 fax
edwardswildman.com

Theodore P. Augustinos
+1 860 541 7710
fax +1 888 325 9082
taugustinos@edwardswildman.com

Via Federal Express and Email
Pam.murphy@doj.nh.gov

February 25, 2013

Attorney General Michael A. Delaney
New Hampshire State Attorney General's Office
33 Capitol Street
Concord, NH 03301

Re: Cartier North America
Notification of Potential Security Breach pursuant to N.H. Rev. Stat. § 359-C.20

Dear Attorney General Delaney:

We write to advise you of an incident involving the loss of a laptop computer, which resulted in the potential compromise of the personal information of one New Hampshire resident. The incident occurred in Boston, Massachusetts on January 18, 2013. To our knowledge, the laptop contained, among other things, certain personal information of 13 U.S. residents, one of whom is a New Hampshire resident.

Learning About the Incident. An employee of Cartier North America (the "Company") inadvertently left his Company laptop in a taxi on January 18, 2013. The laptop was password protected, but it was not encrypted. The Company has not been able to recover the laptop to date. The Company had policies in place prior to this incident prohibiting employees from storing or maintaining personal information on unencrypted laptops, and from storing credit card information on any laptops. Upon learning of this incident, the Company engaged an outside forensic investigation firm to review a recent backup and confirm whether the laptop contained any personal information. On the evening of February 11, 2013, the forensic firm confirmed that the laptop contained the name of one New Hampshire resident along with his credit card number.

At this time, we have no knowledge that any information contained on the laptop was accessed or misused as a result of this incident. The laptop was equipped with a tracking device that would be triggered if the stolen laptop were connected to the Internet, and the device has not been triggered to date.

Upon discovery of the incident, the Company took the following actions: (i) made significant efforts to recover the lost laptop; (ii) engaged our law firm to oversee forensics, coordinate

appropriate data breach response, and advise on legal obligations under applicable law; and (iii) engaged a third party forensic firm to investigate the incident and determine what information may have been compromised by the loss.

Communicating with Affected Individuals. In order to ensure that the affected New Hampshire resident may take steps to protect himself from possible identity theft or other monetary damage, the Company will provide notice regarding this incident via Federal Express on or about February 26, 2013. The notification materials, a template of which is enclosed with this letter, advise customers to remain vigilant by reviewing account statements and monitoring free credit reports. The notification materials also describe the services the Company has made available to affected individuals through Kroll Advisory Services for two years at no cost to them.

Efforts to Deter Future Breach. To supplement the Company's policy restricting the storage of personal information on unencrypted laptops, the Company was in the process of encrypting Company laptops prior to this incident. The timetable for completing this project has been accelerated following the incident. Additionally, the Company has intensified its efforts to implement a global information security awareness program with initial focus on an e-learning PCI-DSS compliance training in North America.

* * * * *

We trust that this letter and its enclosure provide you with the information required to assess this incident and the Company's response. Please let us know if you have any questions or if we may be of further assistance.

Sincerely,

Theodore P. Augustinos

Enclosure

[Cartier Letterhead]

[Date]

[Name]
[Address 1]
[Address 2]

Re: Important Notice Regarding Credit Card Account Ending in [####]

Dear [Name]:

As a valued client of Cartier North America ("Cartier"), the privacy of your information is important to us. We are writing to let you know about a data security incident that involved some of your personal information. Although to date we have no indication that your information has been misused or improperly accessed, we are making you aware of this security incident and our ongoing efforts to safeguard your personal information.

By way of background, a laptop containing some of your personal information was lost by an employee of Cartier on January 18, 2013. Unfortunately, the information contained on the laptop included your name and the account number of your credit card identified above, which you at one point in time supplied to Cartier. While this incident affected only thirteen individuals, rest assured that we are taking appropriate steps to address the incident, and that we are committed to safeguarding all of the information you have entrusted to us.

Upon learning of the accidental loss of the laptop, Cartier immediately contacted law enforcement and forensic investigators, and in addition to conducting a thorough review of the potentially affected records, we have also conducted an investigation surrounding the loss of the laptop and have made attempts to try to locate it. In addition, Cartier has taken steps to further strengthen its security measures to prevent a recurrence of this unfortunate incident, including supplementing our information security policies and staff training program.

We recommend that you remain vigilant and review your account statements and credit reports regularly. To assist you in protecting yourself against risks related to this incident, we have engaged Kroll Advisory Solutions to provide you with its **ID TheftSmart™ program,** which include **Continuous Credit Monitoring, Current Credit Report, idIntegrity Scan** and **Enhanced Identity Theft Consultation and Restoration**. These services are offered for two years at no cost to you. Enclosed with this letter is information regarding these services and instructions for enrollment. To enroll in these services, please follow the enclosed instructions and refer to the ID TheftSmart membership number provided on the second page of this letter.

Cartier deeply regrets that this accident occurred and we sincerely apologize for any inconvenience or concern this may cause you. We are available to answer any questions or concerns you may have and therefore, please do not hesitate to contact Mercedes Abramo, V.P. of Retail for Cartier, at [Telephone number].

Yours sincerely,

Emmanuel Perrin
President and CEO
Cartier North America

Enclosures

Please refer to this number when enrolling for the services referenced above.

ID TheftSmart membership number: [#]

What Should You Do If You Have Any Questions Or Feel You Have An Identity Theft Issue?

Call [Telephone number], 8 a.m. to 5 p.m. (Central Time), Monday through Friday. Kroll's Licensed Investigators are standing by to answer your questions or help you with concerns you may have. *Please have your membership number ready.*

Your Complimentary Identity Theft Protection Services

Current Credit Report

Verify your Credit File is Accurate

Receive an up-to-date credit report giving you a detailed account of your credit activity. If you see any suspicious activity, your licensed investigator is ready to help you.

Experts recommend you review your credit on a regular basis. This is because it can be used to establish a baseline for detecting and safeguarding against identity theft.

Go to **www.idintegrity.com** to order your complimentary **Credit Report**.

Continuous Credit Monitoring

Early Detection is Key

Consumer and government agencies recommend that you keep a close eye on your credit activity. Frequent monitoring is key to identifying fraud and reducing the damage it can cause. Monitoring alerts make you aware of changes in your credit file that could indicate identity theft and fraud.

You'll be notified by email when your credit files are updated with certain credit activity that could be associated with identity theft, such as applying for a new credit card or loan, a change of address, and more.

If any activity looks suspicious, simply call us toll-free. We'll immediately put you in touch with your licensed investigator to find out what's happening and help take measures to correct the problem. We'll even send you notices when there's been no activity in your credit file, so you always know your credit is closely monitored.

Go to **www.idintegrity.com** to start your complimentary **Credit Monitoring**.

idIntegrity Scan

Your Eye on the Internet

Are your Social Security number, credit card numbers, or other personal information appearing on the Internet? Your idIntegrity Scan service gives you insight into your online personal information and provides 24x7 real time fraud detection. idIntegrity Scan searches for your personal information in internet directories, hacker chatrooms, and public and private databases. You'll receive an email alert within minutes whenever your personal information is detected. If the activity is suspicious, your licensed investigator is ready to help you.

As an additional security measure, you will receive access to the Fraud Detection Dashboard—a secure website that rates the potential risk to your identity from "low" to "highest". Your Dashboard gives you up-to-date status reports on your Social Security number, debit and credit cards, postal and email addresses, and phone numbers.

It's easy to start. **Visit www.idintegritySCAN.com**, tell us what information you want monitored, and idIntegrity Scan does the rest.

Enhanced Identity Theft Consultation and Restoration

Restore Your Credit, Regain Your Peace of Mind

You can rely on the expertise of a specialized team of investigators to help search out suspicious activity and fight back against the evolving tactics used by identity thieves. Our licensed investigators have thousands of hours of experience working with and utilizing the laws, regulations, and investigative techniques used for identity theft restoration.

Our consultation services allow you to minimize your risk if your personal data has been compromised. Our tenured investigators can give you personal one-on-one consultation on how best to reduce your identity theft risk. Additionally, if you are a victim of identity theft, we provide full-service restoration, which means experienced licensed investigators do the heavy lifting to restore your identity on your behalf. And since one dedicated investigator is assigned to your case, you can rest assured you will receive the individualized, personal support that is critical to recovering from identity theft.

You now have easy access to the resources you need to search out suspicious activity and to fight back if you have been exposed to the threat of identity fraud. Our in-depth investigations explore:

- Criminal data at federal and state levels;
- State department of motor vehicles (DMV) records;
- Public records, where liens or bankruptcies could surface;
- Social Security tracing, for fraudulent address or status entries;
- Watch lists familiar to the security industry; and more.

If you have an identity theft issue or if you have any questions, call us today using the toll-free telephone number listed in the accompanying letter. Your licensed investigator is ready to help you.

Restoration Service Exclusions

Legal remedy. Any Stolen Identity Event where the victim is unwilling to prosecute the person who caused the victim to suffer the fraud or its consequences.

Dishonest acts. 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.

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

Pre-existing stolen identity event limitations. A pre-existing identity event (occurring prior to and not in any way related to the current breach event) or the consequences caused by it are not covered.

Minors. Minors are fundamentally excluded given that (a) credit reporting agencies do not knowingly maintain credit files on minor children, and (b) minor children are unable to execute the Limited Power of Attorney required for certain restoration processes. However, Kroll will try to resolve identity theft issues for participating minors through the means available under existing legislation and established industry and organizational procedures, with reasonable efforts to address the challenges of working with minors.