Quantum

Quantum Corporation
Corporate Legal Department
1650 Technology Drive, Suite 800
San Jose, CA 95110
www.quantum.com

lisa.glover-gardin@Quantum.com
408 944-4464

June 17, 2010

Sent via E-mail

Ms. Mary Thayer
Consumer Protection & Antitrust Bureau
Attorney General Department of Justice
33 Capitol Street
Concord, NH 03301

Subject: Notice Regarding Potential Unauthorized Access of Customer Information pursuant to NH Rev. Stat. § 359-C:20

Dear Ms. Thayer;

We are writing to inform you of a theft of laptops from the Company's Bellevue, Washington offices. The information contained on one of these laptops included sensitive personal information (SPI) of certain Quantum employees, including four [4] New Hampshire residents. We do not have any evidence that, beyond this theft, this data has been further accessed, used or disclosed but the laptops have not been recovered. We are providing you this advance notice pursuant to § 359-C:20 and in order to alert you to the possibility of attempted identity theft; nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and any steps the Company is taking to restore the integrity of the system.

On the evening of Sunday, June 13, there was a break in at the building in Bellevue, Washington that Quantum partially occupies. The break in was discovered the following day, June 14, by the property manager. We believe that all of the building's tenants were affected, but the Quantum property stolen included mainly electronic equipment, including some laptops taken from the IT work room. Although the laptop containing SPI continued to retain password protection, the theft occurred before the encryption software could be reinstalled. The nature of the crime suggests that data was not the target but rather technology equipment, including: monitors, cables and video conferencing equipment.

Quantum is working diligently with in-house and outside resources to evaluate our physical and data security processes. Quantum is also reviewing IT repair work processes in order to help prevent this type of incident from occurring again.

On June 17 Quantum notified all impacted employees, including the four New Hampshire residents impacted. A copy of the proposed communication is attached. (Please reference Proposed Notification Letter to Impacted Persons per Exhibit A) To further minimize the impact to its employees, Quantum has set up a credit monitoring service for a term of one [1] year to be provided at no cost to all impacted persons.

Should you have any questions regarding the incident giving rise to this notice, Quantum's remedial measures or the proposed notice, please contact me at your earliest convenience. We look forward to working with you to ensure that Quantum's process in compliance with § 359-C:20.

Sincerely,

Quantum Corporation

Lisa Glover-Gardin, Esq.
Senior Consulting Counsel

Attachments:
Exhibit A – Proposed Notification Letter to Impacted Persons

Exhibit A

Quantum

Quantum Corporation
1650 Technology Drive, Suite 800
San Jose, CA 95110
www.quantum.com
408 944-4000

<date>

<name>
<title>
<address>
<city, state, zip>

Subject: Notice Regarding Unauthorized Access of Customer Information

Dear <name>:

Quantum values your privacy and the security of your personal information and has processes and procedures in place to protect it through our Privacy Management Program and Written Information Security Program. Unfortunately, due to a break-in at our Bellevue office, it is possible your sensitive personal information may have been compromised. As a precautionary measure, we wanted to let you know what happened and explain the actions we are taking in response.

On the evening of Sunday, June 13, there was a break in at the building in Bellevue, Washington that Quantum partially occupies. We believe that all of the building's tenants were affected, but the Quantum property stolen included mainly electronic equipment, including some laptops taken from the IT work room. One of these laptops contained employee sensitive personal information, including names, addresses, and Social Security numbers. While that laptop had been encrypted in accordance with Quantum's privacy practices, the software had been temporarily disabled to allow laptop repair. Although the laptop continued to retain password protection, the theft occurred before the encryption software could be reinstalled.

Quantum deeply regrets that this incident occurred, is working with the appropriate law enforcement agencies to investigate the break-in, and will notify you of any significant further developments that impact you. In the interim, Quantum is reviewing its security procedures to evaluate the opportunity to take additional actions we might take to prevent a similar security breach in the future. While we have no indication so far that the information has actually been accessed or used for identity theft purposes, we are working with TransUnion, a major credit monitoring service, to provide the following at no cost to you:

- A one-year subscription to TransUnion 3-Bureau Credit Monitoring Service.
- One year of monthly 3-in-1 credit report updates.
- A one-year subscription to TransUnion's TrueCredit Lock service.
- One year of $25,000 of identify theft insurance coverage with no deductible.

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) regarding steps you can take to protect your information and how to receive free credit monitoring for one year.

For further information and assistance, please contact Quantum's privacy resources at internationalprivacy.officer@quantum.com.

Sincerely,

Rick Belluzzo
CEO and Chairman of the Board

EXHIBIT A
STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834

- **Fraud Alert**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information below:

Equifax	Experian	TransUnion
(877) 576-5734	(888) 397-3742	(800) 680-7289
www.alerts.equifax.com	www.experian.com/fraud	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834

Additional information is available at http://www.annualcreditreport.com.

- **Credit Report Monitoring**

In addition to the services noted above, Quantum has arranged with TransUnion to provide you with credit monitoring for one year, at no cost to you. This service provides you with the following benefits at no cost to you:

- A one-year subscription to TransUnion 3-Bureau Credit Monitoring Service.
- One year of monthly 3-in-1 credit report updates.
- A one-year subscription to TransUnion's TrueCredit Lock service.
- One year of $25,000 of identify theft insurance coverage with no deductible.

To take advantage of this offer, you must enroll by September 30, 2010.

To enroll in this free service, go to TrueCredit by TransUnion web site at www.truecredit.com/code and in the space referenced as gift certificate code, enter **[Insert 16-digit Gift Certificate Code]** and follow the simple steps to receive your free products online within minutes. These services are only available to Quantum employees impacted by the laptop theft, so this code should not be shared with others.

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift or remove the security freeze.

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

In addition, Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.stat.md.us, or calling 1 (888) 743-0023.