Weil, Gotshal & Manges LLP

767 Fifth Avenue
New York, NY 10153-0119
+1 212 310 8000 tel
+1 212 310 8007 fax

Bruce A. Colbath
+1 (212) 310-8590
bruce.colbath@weil.com

May 28, 2013

Office of the New Hampshire Attorney General

Dear Attorney General:

We represent Godiva Chocolatier, Inc. ("Godiva"). This letter is intended to notify you of an instance of unauthorized access to electronic information maintained by Godiva that recently came to the attention of the company.

On or around April 15, 2013, Godiva received a letter from a private individual's counsel alerting Godiva that the individual's son found a flash drive in New York City that appeared to contain sensitive information about Godiva. At Godiva's request, the individual promptly returned the flash drive to Godiva with the drive contents apparently intact. Subsequently, and at Godiva's request, both the lawyer and the individual who returned the flash drive confirmed that, to their knowledge, no one had copied or otherwise improperly used any of the information contained on the flash drive.

Godiva immediately undertook an investigation into the cause and the scope of the incident. By working with a third-party, forensic investigator (Navigant Consulting, Inc., "Navigant"), Godiva was able to confirm that the information on the flash drive was accessed on April 1, 2013, which aligns with the account given by the individual. Upon further investigation, Godiva learned that a one-time Godiva employee, with authorized access to certain human resources information and apparently acting within the scope of the employee's employment, had compiled, among other company information, certain employment data on the flash drive. It is believed that this employee lost the flash drive on or around Lexington Avenue in New York City.

The flash drive contained human resources data for certain Godiva job applicants and employees who worked at Godiva or applied for positions at Godiva prior to August 5, 2010. Navigant has determined that the personal information stored on the flash drive includes employee Social Security numbers, dates of birth, addresses, phone numbers, resumes, photos, and Employee ID numbers.

Based on Godiva's investigation and the forensic examination of the flash drive conducted by Navigant, Godiva has no reason to believe that anyone, other than the aforementioned individual and his son, had unauthorized access to this information. There is no evidence that any of the information contained on the flash drive was downloaded or copied by others. Godiva's investigation has not uncovered any evidence that the information was used improperly or involved any criminal conduct, nor have there been any reports of suspected identity theft. Moreover, in light of the representations by

the individual whose son found the flash drive and his counsel, there is no reason to believe the data will be misused in the future.

Nevertheless, out of an abundance of caution, Godiva is in the process of providing written notice to all persons who might have been affected, including residents of states where notice under these circumstances may not otherwise be required. Godiva worked with Navigant to identify all Godiva job applicants and Godiva current and former employees (and any other individuals, such as spouses) whose personal information was inadvertently accessed. This event does not affect Godiva customers, since no customer information was saved to the recovered flash drive.

In addition to notifying all relevant Godiva job applicants and current and former employees and the relevant state authorities, Godiva is also notifying the major consumer reporting agencies to alert them to the inadvertent disclosure of personal information.

In actions unrelated to the creation of the flash drive involved in this incident, and the recent notification to Godiva that the flash drive was found and accessed by an unauthorized individual, Godiva had already previously modified its data security policies applicable to its electronic resources (the Godiva "Acceptable Use Policy"), to mandate additional security controls and privacy measures to prevent unauthorized access to confidential information. In an effort to prevent any future incidents of this type, Godiva specifically prohibits any employee from accessing data without appropriate authorization and from duplicating confidential data to portable media devices without appropriate safeguards, including password protection and encryption, to ensure continued confidentiality of all data.

Godiva estimates that approximately 101 affected persons are residents of your state and will be notified pursuant to the laws of your jurisdiction. Notification of the unauthorized access is to be provided, via first class mail, to all affected employees on or around May 29, 2013. A copy of the notification is attached. As described in the resident notification letter, Godiva is providing free credit monitoring services to all notice recipients who wish to enroll. Godiva has also established a toll-free confidential assistance telephone line to utilize if individuals have any questions or concerns regarding the incident described in their notification letter. This line is staffed with outside professionals trained in identity protection and recovery assistance. This line can be reached Monday through Friday, from 9:00 a.m. to 9:00 p.m. E.S.T. by dialing, toll-free, 1-877-797-6091.

Please refer any questions to:

Jonathan D. Drucker, Esq.
Senior Vice President and General Counsel
Godiva Chocolatier, Inc.
333 West 34th Street
New York, NY 10001
Tel. 212-984-5900

Email: jonathan.drucker@godiva.com

or

Bruce A. Colbath, Esq.
Weil, Gotshal & Manges LLP
767 Fifth Avenue
New York, NY 10153
Tel. 212-310-8590

Email: bruce.colbath@weil.com

Sincerely,

Bruce A. Colbath

Godiva
PO Box 6336
Portland, OR 97008

May 29, 2013

Name
Address 1
Address 2
City, State Zip

Dear Name,

On April 15, 2013, Godiva received a letter informing us that an individual, without authorization, had obtained and accessed a flash drive containing certain personal information about some individuals who worked at Godiva, or applied for positions at Godiva, prior to August 5, 2010. The information accessed varies from individual to individual, but could, in some cases, include names, addresses, social security numbers, phone numbers, and other information related to employment records at Godiva.

The flash drive was returned to Godiva on April 19, 2013, and Godiva has been assured by the individual who provided it to Godiva that the information contained on the flash drive was not copied. We have no reason to believe that any of your personal information was copied, nor do we have any information that it was used improperly. Nevertheless, out of an abundance of caution, we are notifying you of the incident and the steps you can take to monitor the security of your identity and personal information. We are also offering you, at Godiva's expense, the opportunity to have your credit monitored by an outside identity protection agency. Please see the attached page for details.

We regret that this incident has occurred and want to emphasize that Godiva takes this matter and the security and protection of your personal information very seriously. Since the time that this information was compiled on the flash drive several years ago, Godiva has implemented additional security and access controls for electronic resources in an effort to further minimize the risk of unauthorized access to confidential information. Godiva specifically prohibits any employee from accessing data without appropriate authorization and from copying confidential data to portable media devices without appropriate safeguards, including password protection and encryption to ensure continued confidentiality of all data.

We have established a toll-free confidential assistance telephone line to help answer any questions you may have regarding the incident described in this letter. This line is staffed with outside professionals trained in identity protection and recovery assistance. This line can be reached Monday through Friday, from 9:00 a.m. to 9:00 p.m. E.S.T. by dialing, toll-free, 1-877-797-6091.

We regret any inconvenience this incident may have caused you and again emphasize that we have no reason to believe that your personal information was either copied or used improperly.

Sincerely,

Kristine Breuer, Senior Vice-President Global Human Resources

Recommended Steps to Help Protect Yourself

As always, we encourage you to remain vigilant in guarding your personal information, to carefully review your credit card or other financial account statements, and to monitor your credit reports for any suspicious or unauthorized activity. You may also wish to do the following:

months of your credit report from each of the three major credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling, toll free, 1-877-FACTACT (1-877-322-8228). You may also contact the three major credit reporting agencies directly to request a free copy of your credit report.

- Contact the major credit reporting agencies: To further protect yourself, you may contact the fraud departments of each of the three major credit reporting companies. They will discuss your options with you and provide information on fraud alerts, security freezes, and other steps you can take to protect yourself from fraud and identity theft.

  - Place a security freeze: A security freeze is designed to prevent credit, loans, and services from being approved in your name without your written consent. However, using a security freeze may delay your ability to obtain credit.

  - Place a fraud alert: A fraud alert indicates to a business that your personal information might have been compromised and requires the business to take additional steps to verify your identity before issuing you credit. For that reason, placing a fraud alert on your account(s) can protect you, but also may delay your ability to obtain credit. You have the right to ask that the three credit reporting companies place fraud alerts in your file, at no charge. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting companies. As soon as one credit bureau processes your fraud alert, it will notify the other two credit reporting companies which then must also place fraud alerts in your file.

  - To place a fraud alert or security freeze, or should you have any questions regarding your credit report, you can contact the major credit reporting agencies directly at:

Equifax	Experian	TransUnion
1- 800-685-1111 (general)	1-888-397-3742	1-800-680-7289
1-800-525-6285 (fraud hotline)	www.experian.com	www.transunion.com
www.equifax.com		

- Enroll in a free credit-monitoring program: We have arranged for you to receive identity theft protection services through ID Experts, the data breach and recovery services expert, to provide you with FraudStop Credit Edition at no cost to you.

  - ID Experts' fully managed recovery services will include: (1) 12 months of credit monitoring; (2) $20,000 insurance reimbursement policy; (3) exclusive educational materials; and (4) access to fraud resolution representatives.

  - With this protection, ID Experts will help you resolve issues if your identity is compromised. We encourage you to contact ID Experts with any questions and to enroll in the free services by calling the toll free assistance line at 1-877-797-6091 from Monday through Friday, from 9:00 a.m. to 9:00 p.m. E.S.T. or by going to www/.idexpertscorp.com/protect.

  - **Your membership code for this free credit-monitoring program is: [MEMBER ID]**

- Further educate yourself regarding identity theft: You can learn about the steps you can take to protect yourself by contacting your state Attorney General or the Federal Trade Commission (FTC).

- Contact the FTC: The FTC provides useful information about identity theft and maintains a database of identity theft cases for use by law enforcement agencies. To file a report with the FTC, you can call the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); send a written report to: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580; or visit: www.ftc.gov/bcp/edu/microsites/idtheft/.

- Report any instances of known or suspected identity theft to law enforcement.

You can obtain additional information about the steps you can take to protect yourself by contacting the following:

For North Carolina Residents:
Office of the Attorney General of North Carolina
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400; 1-877-566-7226

For Maryland Residents:
Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
www.oag.state.md.us
Telephone: 1-888-743-0023

For Oregon Residents:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/bcp/edu/microsites/idtheft/
1-877-IDTHEFT (438-4338)