BIMBO BAKERIES USA

255 Business Center Drive
Horsham, PA 19044

H.P. BAKER
Attorney
Legal Department
Phone: (215) 323-9242
Fax: (215) 293-9629

May 2, 2012

Department of Justice
Consumer Protection Bureau
33 Capital Street
Concord, NH 03301

RE: Notice of Potential Data Breach Pursuant to NH Rev. Stat. § 359-C:20

To Whom It May Concern:

I am writing to notify you that a computer assigned to one of our associates was stolen from the trunk of his car. After investigating the incident, we believe the computer contained a spreadsheet whose content included personal information including the names and social security numbers of 22 New Hampshire residents who are current or former associates. This information was properly on the computer for business related purposes.

After we learned of the theft, we instituted the following:

1. The theft was reported to local authorities on April 14, 2012.
2. We promptly undertook measures to determine what personal information was on the laptop.
3. We are sending notification letters via first-class mail, return receipt requested to any individual believed to have appeared on the spreadsheet in question. (A copy of the notification letter is enclosed).
4. Associates are being offered 12 months of identity theft monitoring free of charge.

More details regarding the potential breach can be found in the attached letter being sent to the affected individuals this week.

Bimbo Bakeries, USA is committed to maintaining and protecting the confidentiality of our associates' personal information. We regret that this situation has occurred and will be working to reduce the risks of a similar situation happening in the future.

If you have any questions, please feel free to contact me.

Very truly yours,

H.P. Baker

BIMBO BAKERIES USA

Christine Ammon
Director, Human Relations
Phone: (518) 373-2827 ext. 18

CERTIFIED MAIL - RETURN RECEIPT REQUESTED

May 1, 2012

Re: Theft of BBU Computer

Dear Amanda:

We are writing to inform you that a computer issued to an associate working for Bimbo Bakeries USA ("BBU") that contained some information about you was recently stolen. While we have no reason to believe that any of that information has been accessed without authorization or has been or will be used in any unauthorized way, we are writing to tell you what happened, what we have done to address the situation, and what you can do to protect your continued privacy. I also attached a reference guide that contains useful information.

What Happened

We believe that the stolen computer contained files that included personal information about you. This information included your name and social security number. This information was properly on the computer for business related purposes. Once discovered, we promptly reported the theft to local authorities. We also immediately disabled the login credentials associated with this computer so that it cannot be used to access any additional information about you that may reside on our network. Again, we do not know, or have reason to believe, that the thief has in fact accessed your name and social security number, that such information has been or will be used improperly, or that your information was targeted for criminal or inappropriate purposes.

What We Are Offering

As a free service, BBU has arranged for you to receive identity theft monitoring for 12 months. If you would like to enroll in the program, please send a letter to Catherine Kenny informing her of your desire to enroll. Your letter should be sent to

Catherine Kenny
Bimbo Bakeries, USA
255 Business Center Drive
Horsham, PA 19044

Your letter must be received by May 21, 2012. Upon receipt of your letter, Catherine will provide you with additional details about registering for the monitoring service.

What You Can Do

In addition to the above-described program that BBU will provide to you free of charge, there are three simple steps you can take to protect your continued privacy and be sure that the stolen information is not used improperly, both of which are good practices in any event.

First, monitor your credit report to be sure that credit is not being established in your name and social security number without your authorization. You can do this by obtaining a free credit report by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or completing the 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 the form from http://ftc.gov/bcp/conline/pubs/credit/freereports.pdf or contact me for a copy. If at any time you feel it is necessary, you can also place a fraud alert or freeze on your credit file with the major credit reporting agencies by contacting any one of them as indicated on the enclosed form.

Second, take steps to prevent unauthorized access to any accounts you have with any financial institution. This includes bank accounts, credit cards, brokerage accounts, etc. You should notify each such financial institution that a computer which contained your name and social security number was stolen. Based on the nature of your account and the information you use to access it, the financial institution may suggest additional steps. Also, and perhaps more importantly, **you should check your periodic statements from each such financial institution promptly upon receiving them to be sure that no unauthorized transactions have occurred**.

Third, if you use your name and social security number as a login name or password in any way, you should take the steps necessary to change it to something else. For example, if you have online accounts at websites that require a login name or a password and you use your name and social security number for either, you should change it.

If you find any suspicious activity on your credit report or at any of your financial institutions, notify the financial institution or credit agency immediately. Under U.S. federal law, consumers are liable only for the first $50 of any fraudulent charges made on their credit or bank accounts, but only if such charges are reported promptly in writing to the appropriate financial institution after a statement is provided to you. Protect yourself by reviewing statements carefully and promptly reporting any unauthorized activity. You should also call your local police or sheriff's office to file a police report of any unauthorized activity you discover. Obtain a copy of the police report for your records and future reference.

For general information on protecting your privacy and preventing unauthorized use of your personal information, we suggest you contact your state office of consumer affairs or attorney general or visit the U.S. Federal Trade Commission's Web site, http://ftc.gov.

We are committed to maintaining the privacy of the personal information you entrust to us. We apologize for any inconvenience or concern this incident may cause. If we can be of any further assistance or answer any questions, or you encounter any problems that you believe to be related to this incident, please call me directly.

Sincerely,

Christine Ammon
Director, Human Relations

Reference Guide

In the event that you ever suspect that you are a victim of identity theft, we encourage you to consider taking the following steps:

Contact the Federal Trade Commission. You can contact the Federal Trade Commission's Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC, 20580 or at http://www.ftc.gov/bcp/menus/business/data.shtm, to obtain more information about steps you can take to avoid identity theft.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

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 a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze by contacting the credit bureaus at:

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	www.transunion.com

The credit bureaus may charge a reasonable fee to place a freeze on your account, and may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to

provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. 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 Federal Trade Commission ("FTC"). If you believe you identity has been stole, 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 learn more about how to protect yourself from becoming an identity theft victim of by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)

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

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5 each to place, temporarily lift, or permanently remove a security freeze.

For North Carolina Residents: You can obtain information from the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact Attorney General Roy Cooper's Consumer Hotline toll-free within North Carolina at 1-877-5-NO-SCAM or (919) 716-6000.