Mondelez Global LLC
3 Parkway North, Deerfield, IL 60015

T. (847) 943 4000
Mondelezinternational.com

NOTICE OF DATA BREACH (NEW HAMPSHIRE)

August 16, 2018

VIA ELECTRONIC MAIL

TO: Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Dear Attorney General:

We are writing to notify you of a breach of security involving New Hampshire residents. Information regarding the breach is provided below and a copy of the notice sent to affected New Hampshire residents is attached to this letter.

If you have any questions or need any help with anything mentioned in this letter, please contact me by e-mail or by phone at the contact information provided below.

Respectfully,

Jeff Srulovitz
VP & Chief Business Integrity Officer and Head of Global Security

Name & Contact Information of Person Reporting Breach	Jeff Srulovitz VP & Chief Business Integrity Officer and Head of Global Security Mondelēz Global LLC 3 Parkway North, Deerfield, IL 60015 847-943-4354 jsrulovitz@mdlz.com
Name & Address of Business Experiencing Breach	Mondelēz Global LLC 100 Deforest Avenue East Hanover, NJ 07936
Business Type	Commercial (confectionery, food, and beverage company)

Date(s) of Breach	July 24 and July 26, 2018
Description of Breach	An unauthorized and fraudulent email (phishing attempt) was sent by a third party to Mondelēz employees asking recipients to complete a survey that required employees to provide their Mondelēz usernames and passwords. If an employee provided their username and password, the perpetrator used the credentials to gain, or attempt to gain, unauthorized access to the employee's UltiPro payroll account and Microsoft email account.
When/How Breach Discovered	July 29, 2018 We discovered the breach
Remedial Steps Taken	▸ Restricted access to those online accounts which we know were impacted. ▸ Took steps to ensure that all employees changed their online passwords immediately. ▸ Deleted unopened copies of phishing messages from the system and mailboxes, removed MS Outlook "rules" that had been added by the malicious actors, and restored information that had been modified. ▸ Flagged and are continuing to monitor all impacted accounts to prevent any further unauthorized account changes. ▸ Notified law enforcement
Personal Information Subject to Breach	▸ Employee name ▸ Username and password (used to access payroll account and Microsoft email account) ▸ Bank account number and routing information ▸ W-2 information (including *Social Security Number* if contained in W-2)
# of Residents (*in State*) Affected	One
Date(s) Notification Sent to Individuals & Notification Method	August 14, 2018 Email
Credit monitoring or identity theft protection services offered to affected residents?	☐ No ☒ Yes *Description*: Experian IdentityWorks Premium (provides Identity Theft Monitoring & Protection, Credit Lock, and Credit Monitoring and Alerts) *Length*: 12 months
Notification delayed due to a law enforcement investigation?	☒ No ☐ Yes
Template copy of notification sent to affected individuals attached?	☐ No (*not required/requested*) ☒ Yes

Mondelez Global LLC
3 Parkway North, Deerfield, IL 60015

T. (847) 943 4000
Mondelezinternational.com

August 16, 2018

[FName] [LName]
Via e-mail

Dear [FName]:

Mondelēz Global (MG) recently became aware that some of your personal information may have been inappropriately accessed or used by a third party who obtained your MG login credentials through a phishing attack. The perpetrators may have accessed or otherwise obtained your name, MG username and password, and other information maintained by you in the UltiPro payroll system.

Specifically, our investigation has revealed that on or about July 24 and 26, a phishing email was sent by a third party to MG employees asking recipients to complete a survey that required employees to provide their usernames and passwords. If an employee provided their username and password, the perpetrators used the credentials to gain, or attempt to gain, unauthorized access to the employee's UltiPro payroll account, MG email account, and other applications. Once the perpetrators were able to gain access to these accounts, they were able to view your contact information, bank account numbers, basic employment and income information, W-2 information (including your Social Security number if contained therein), and any other information visible through your UltiPro account.

Once we learned of the breach, we restricted access to those online accounts which we know were impacted – including yours – and took steps to ensure that all employees changed their passwords immediately. In addition, we restored the information in your accounts back to the way they were prior to the attack and flagged and are continuing to monitor all impacted accounts to prevent any further unauthorized account changes. **If you have not changed your login password used to access the MG computer network, please do so immediately**.

To protect yourself from potential harm resulting from the breach we encourage you to closely monitor all of your personal financial information and accounts, all mail (electronic or printed), phone calls or other contact from individuals not known to you personally, and avoid answering any questions or providing additional information to those individuals.

Further, because it is important to remain vigilant for incidents of fraud and identity theft, we are offering a *complimentary* one-year membership with Experian's® *IdentityWorks*^{SM}. This product, paid for by MG, helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. These are the details:

- To sign up visit the Experian website: www.experian.com or use this link. You can also contact Experian by phone at 866-617-1922.

- Provide your activation code: [ ]
- Please ensure to enroll by [ ] (Your code will not work after this date).

If you have questions about the product, need assistance with identity restoration, please contact Experian's customer care team at [customer service number] by **[enrollment end date].** Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

In addition, you can obtain a free copy of your credit report and information about fraud alerts and security freezes by contacting any of the three credit reporting agencies listed below. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts 90 days, after which you can renew it by calling the credit reporting agency again. Once you place the fraud alert with one of the three agencies, they will alert the other two. In addition, you may have a right to a "security freeze." A security freeze completely blocks the information on your credit report from would-be creditors. Please contact one of the below credit reporting agencies for more information. The relevant contact information for each of the agencies is as follows:

Equifax	**Experian**	**TransUnion**
Credit Report: 800-685-1111	Credit Report: 888-397-3742	Credit Report: 877-322-8228
Fraud Alert: 888-766-0008	Fraud Alert: 888-397-3742	Fraud Alert: 800-680-7289
Security Freeze: 800-685-1111	Security Freeze: 888-397-3742	Security Freeze: 888-909-8872
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000

Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year.

For more information on steps you can take to protect yourself from identity theft or to report identity theft matters, you can also contact the Federal Trade Commission's identity theft hotline at 1-877-ID-THEFT (1-877-438-4338), or by visiting the Federal Trade Commission website at www.ftc.gov/idtheft, or writing to the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. In addition, if you discover any suspicious activity on your accounts, notify law enforcement or your state Attorney General's office immediately.

If you have any questions, please feel free to contact John Hines, the MG HR representative who is prepared to answer any questions you may have. He can be reached at 847-943-4300, or by email at john.hines@mdlz.com, or by writing to the address contained in the letterhead.

Very truly yours,

John Hines
Associate Director HR Solutions NA