HILL+KNOWLTON
STRATEGIES

OFF OF THE ATTY GENERAL
2016 MAY 11 P 12:48

825 Third Avenue
Suite 2400
New York, NY 10022

Mr. Brian Frosh
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202-2202
Attn: Security Breach Notification
Idtheft@oag.state.md.us

April 29, 2016

Dear Attorney General Frosh,

Please be advised that on February 23, 2016, an employee of Hill+Knowlton Strategies sent certain employee records to an unauthorized email recipient. The incident was not discovered until Friday, April 22, 2016. The documents contained certain personal information of Hill+Knowlton Strategies employees including names, home addresses, social security numbers and salary information.

It appears that 592 individuals could have been affected, including 20 individuals who are residents of your state. A draft copy of the notification letters being sent to the affected individuals is attached.

As set forth in the letter, we have taken numerous steps to protect the security of the personal information of the affected individuals, including implementing additional quality controls to avoid similar incidents in the future.

If you have any questions, please contact me at 212-885-0300 or email Mike.coates@hkstrategies.com.

Sincerely,

Mike Coates
President and CEO, The Americas

[Company Logo]

[Return Address]
[Date]

ANY NAME
ANYSTREET
ANYCITY, ANYSTATE, ZIP

RE: Important Security and Protection Notification
Please read this entire letter.

Dear ANY NAME:

WHAT HAPPENED?
I am writing to let you know that certain personal information of individuals employed within Hill+Knowlton Strategies in the U.S. during 2015 has been compromised. We learned on Friday, April 22, 2016 that we were the target and victims of a sophisticated phishing attack that occurred two months prior. We want to ensure you that we are treating this matter extremely seriously and are working diligently to minimize the impact of this incident. We are giving our response the highest priority and are sincerely sorry for this incident and any inconvenience this may cause you. Please understand that we are all personally in the same situation as you, and are doing our best to manage the situation.

WHAT INFORMATION WAS INVOLVED?
The records were 2015 W2 tax forms which contained your name, home address, social security number and salary information.

WHAT WE ARE DOING.
We take any loss of personal data very seriously and are taking steps to help protect you and your personal information. We have been working with federal and state tax authorities, legal and tax experts, and law enforcement to address and respond to the incident, and I thank you for patience as we work through this.

To help protect your identity, we are offering a **complimentary** two-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. We strongly encourage you to promptly take advantage of this service.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: 07/31/16** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/alert**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide engagement #: **[engagement #].**

Additional details regarding your 24-MONTH ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian credit report.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-297-7780.

WHAT YOU CAN DO.

- **Order Free Annual Credit Reports**
  You have the right to obtain a copy of your credit report for free once a year from each credit reporting agency by contacting one of the agencies listed below or by visiting www.annualcreditreport.com or by calling toll free 877-322-8228. Hearing impaired consumers can access TTY service at 800-821-7232. You may order one, two, or three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the information in your reports.

  Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. The three credit bureaus are:

Equifax	Experian	TransUnion
877-478-7625	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **Place A 90-Day Fraud Alert On Your Credit File**
  You can also place an initial "fraud alert" on your credit file. A "fraud alert" lets creditors know that they should contact you before they open a new account in your name. Additionally, you could also place a security freeze which prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. You can learn more information about placing a fraud alert or security freeze by calling any one of the three credit reporting agencies at the numbers above.

- **Place A Security Freeze On Your Credit File**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

- **Manage Your Personal Information**
  Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

OTHER IMPORTANT INFORMATION.

Social security numbers can be used to open lines of credit or file false tax returns. While taking the steps outlined above can be helpful, and the IRS is aware of common identity theft scams, you should be vigilant in attending to your accounts and financial matters. Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. Report any suspected incidents of identity theft to local police, the Federal Trade Commission and contact a credit reporting company.

The IRS has posted information and procedures regarding how to deal with identity theft with respect to the filing of tax returns, including providing a form (Form 14039) to notify the IRS directly if your efiled Return is rejected because of a duplicate filing under your identity. In the event a fraudulent Return has been filed, you will still be entitled to any refund owed to you (though it may be delayed) but please note that you will not be able to e-file your Tax Return and will need to file a paper Return. Your individual State may have more information regarding State tax returns on their own website. Please see: https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information. If you have filed for an extension and have not yet filed your Return, you are encouraged to file as soon as possible.

FOR MORE INFORMATION.

You can also visit https://www.identitytheft.gov for more information. To contact the Federal Trade Commission or the state attorney general's office you can use the information provided below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/complaint
1-877-382-4357 / TTY: 1-866-653-4261

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
(410) 576-6300 or 1-888-743-0023

Please be assured that we take the protection of your information very seriously. We apologize for any inconvenience this incident may cause you. If you have any questions, please contact Experian's customer care team at 877-297-7780.

Sincerely,

Jill Miller
SVP, US Director of Human Resources

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.