orrick

September 18, 2017

Via Mail

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Orrick, Herrington & Sutcliffe LLP
Columbia Center
1152 15th Street, N.W.
Washington, DC 20005-1706
+1 202 339 8400
orrick.com

Antony P. Kim

E akim@orrick.com
D +1 202 339 8493
F +1 202 339 8500

Re: Notification of Security Incident

Dear Sir or Ma'am:

I am outside counsel to W.W. Grainger, Inc. On behalf of Grainger, please see the following notification regarding a recent security incident. If you have any questions or concerns, please do not hesitate to reach out to me directly via email (akim@orrick.com) or phone (202.339.8493).

Respectfully submitted,

Antony P. Kim
Global Co-Chair, Cybersecurity & Data Privacy
Orrick Herrington & Sutcliffe LLP
office +1 202.339.8493
mobile +1 202.270.7590

NOTIFICATION REGARDING SECURITY INCIDENT

Dear Sir or Ma'am:

W.W. Grainger, Inc. is a B2B provider of MRO (maintenance, repair and operations) supplies, headquartered in Lake Forest, IL. At Grainger, we take privacy and security very seriously, including prompt response to security incidents. I am writing to inform you of a recent matter that may have affected the personal information of approximately 1,056 current and former Grainger employees who are residents of Iowa.

In the early morning hours of August 23, 2017, a Grainger employee was the victim of a crime when his laptop was stolen from his vehicle parked outside his home, located in a Chicago-area transitioning neighborhood. On that same day, the employee reported the theft to police and to the Grainger incident response team. Within hours, we launched an investigation with the assistance of cybersecurity counsel, outside security experts, and in close cooperation with law enforcement. The employees' network and all other IT credentials were disabled, and the laptop was set to automatically wipe its contents the next time it connects to the internet.

The next day, Grainger's loss-prevention team met with local police, and were told that the employee's neighborhood had recently experienced a series of thefts. The team also met with the Chicago police department to initiate an alert on the laptop's make, model and serial number through Chicago PD's pawn-shop tracking system. We remain in contact with and ready to assist law enforcement, and have set up online resources to monitor for any sales offers related to the laptop.

On August 24-25, we analyzed the files on the laptop using system back-ups, and identified personal information belonging to current and former Grainger employees, including names, contact information (such as home address), social security numbers, and retirement benefits information. This personal information varies by individual. We have no reason to believe the criminal knew the type of information on the laptop, and based on our on-going monitoring, we have no evidence that any information has been accessed, viewed or used inappropriately by an unauthorized person The laptop was password-protected, had remote wipe capability, and as noted above, the employee's network credentials were disabled.

Out of an abundance of caution, Grainger is offering 12 months of complimentary identity protection and 12 months of complimentary credit monitoring services to all potentially affected individuals. Information about these services is contained in Grainger's statutory notification letters, a template of which has been attached hereto. Grainger will mail hardcopy notifications during the week of September 18.

If you have any questions, please do not hesitate to reach out.

Respectfully submitted,

Aimee Nolan

Aimee Nolan

Associate General Counsel and Chief Intellectual Property Counsel
W.W. Grainger, Inc.

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

At Grainger, we take privacy and security very seriously, including prompt responses to data breaches. I am writing to you about a recent incident involving personal information of those associated with Grainger.

It is important to note, at this time, based on our on-going monitoring, we have no indication that any personal information has been accessed or viewed by an unauthorized person, or has been used inappropriately. However, out of an abundance of caution, we are notifying all potentially affected individuals.

The facts are summarized below, along with an outline of measures Grainger has taken since discovering the incident. While the company has implemented several protective measures since discovering this incident, it is important that each team member also take appropriate steps to safeguard their sensitive information. This letter provides guidance on general best practices regarding identity theft, as well as information about how to sign up for complimentary identity monitoring services.

What Happened?

On August 23, 2017, Grainger learned that a team member's laptop was stolen. On that same day, as soon as the theft was discovered, Grainger launched an investigation to determine the specifics and information involved. The team member's network and all other IT credentials were immediately disabled, and the laptop was set to automatically wipe its contents completely and permanently the next time it connects to the internet.

We are notifying you because, as someone currently or formerly associated with Grainger (as an employee or dependent of an employee), some of your information is believed to have been on the password protected laptop. It's important to note that we have no reason to believe the criminal knew the type of information on the laptop, and based on our on-going monitoring, we have no evidence that any information has been accessed, viewed or used inappropriately by an unauthorized person. However, we are reaching out so you can take appropriate steps to protect yourself.

What Information was Involved?

The information may have included data such as the following: name, contact information, including home address, Social Security number, date of birth, and employee benefits information. Each individual may have been affected differently.

What Grainger is Doing.

The security and confidentiality of your information is paramount to Grainger. We have been working closely with law enforcement and outside security experts in an effort to find the laptop and apprehend the criminal. We will pursue criminal prosecution to the full extent of the law.

While we have no indication that any personal information has been accessed by an unauthorized person or used inappropriately, as an added precaution, Grainger is providing you with the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has

extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **January 18, 2018** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

What You Can Do.

- We urge you to remain vigilant against threats of identity theft or fraud, and to regularly review your credit card statements and credit reports for any unauthorized activity.
- If you ever suspect that you are a victim of identity theft or fraud, you have the right to file a police report. You also may contact your State Attorney General's office or the Federal Trade Commission to learn about the steps you can take to protect yourself against identity theft. In addition, it's a good practice to change all of your passwords on a regular basis and never use the same password for multiple system logins.
- We are offering you complimentary identity monitoring services, provided by Kroll, a global leader in risk mitigation and response. Please read the following carefully and use these services.

For More Information.

If you have questions or need additional information, please call Kroll toll free at 1-833-202-7407, 8 a.m. to 5 p.m. CT, Monday through Friday.

Grainger is committed to keeping your personal information safe. We sincerely regret any concern or inconvenience this matter may cause you.

Scott Witz

Vice President, Total Rewards & Shared Services

TIPS AND RESOURCES

What Government Agencies Provide Resources?

U.S. Federal Trade Commission (FTC): The FTC has helpful information about how to avoid and protect against ID theft. Write to: Consumer Response Center, 600 Pennsylvania Ave., NW, H-130, Washington, D.C. 20580. Call Toll-Free: 1-877-IDTHEFT (438-4338); or Visit: http://www.ftc.gov/idtheft

State Attorney General Offices: You may contact the Attorney General's office in the state in which you reside for more information about preventing and managing ID theft.

For IOWA Residents: You may contact local law enforcement or the Iowa Attorney General's Office at 1305 E. Walnut St., Des Moines, IA 50319; Tel: (515) 281-5164; or http://www.iowa.gov/government/ag

For MARYLAND Residents: You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202; Tel: (888) 743-0023; or http://www.oag.state.md.us

For NEW MEXICO Residents: You have a right to place a security freeze on your credit report or submit a declaration of removal with a consumer reporting agency pursuant to the Fair Credit Reporting and Identity Security Act. Please see below for more information on security freezes.

For NORTH CAROLINA Residents: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699-9001; Tel: (919) 716-6400; Fax: (919) 716-6750; or http://www.ncdoj.com

For RHODE ISLAND Residents: You may obtain information about preventing identity theft from the FTC or the Rhode Island Attorney General's Office at 150 South Main Street, Providence, RI 02903; Tel: (401) 274-4400; or http://www.riag.ri.gov

How Do I Get A Free Credit Report?

You may obtain one (1) free copy of your credit report once every 12 months, and may purchase additional copies. Call Toll-Free: 1-877-322-8228; or Visit: https://www.annualcreditreport.com; or contact: Equifax, P.O. Box 740241, Atlanta, GA 30374-0241 (800) 685-1111 (www.equifax.com); Experian P.O. Box 2002, Allen, TX 75013, (888) 397-3742 (www.experian.com); TransUnion, P. O. Box 1000, Chester, PA 19022, (800) 888-4213 (www.transunion.com).

What is a "Fraud Alert"?

You may have the right to place a fraud alert in your file to alert potential creditors that you may be a victim of identity theft. Creditors must then follow certain procedures to protect you. You should know that a fraud alert may delay your ability to obtain credit. An "initial fraud alert" stays in your file for at least 90 days. An "extended fraud alert" stays in your file for 7 years, and will require an identity theft report, which is usually a filed police report. You may place a fraud alert by calling any one of the three national consumer reporting agencies: Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-800-680-7289.

What is a "Security Freeze"?

Certain U.S. state laws allow a security freeze, which prevents credit, loans or services from being approved in your name without your consent. A security freeze can interfere with or delay your ability to obtain credit.

To place a freeze, send a request by mail to each consumer reporting agency (addresses below) with the following (for each individual): (1) Full name, middle initial and any suffixes; (2) Social Security number; (3) Date of Birth; (4) proof of current address (such as a utility bill or telephone bill) and list of previous addresses for past five years; (5) copy of government issued ID card, and (6) copy of police report, investigative report or complaint to law enforcement regarding ID theft. You may be charged a fee up to $5.00 to place, lift, and/or remove a freeze, unless you are a victim of ID theft or the spouse of a victim, and you have submitted a valid police report relating to the ID theft incident to the consumer reporting agency. The consumer reporting agencies have three business days after receiving your letter to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you a unique PIN or password that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as

well as the identities of entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The consumer reporting agencies have three business days after receiving your request to lift the security freeze for the identified entities or specified time period.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the freeze. Equifax Security Freeze: P.O. Box 105788, Atlanta, Georgia 30348; Experian Security Freeze: P.O. Box 9554, Allen, TX 75013; TransUnion (Fraud Victim Assistance Division): P.O. Box 6790, Fullerton, CA 92834-6790.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.