

# **Exhibit A**



February 27, 2018

## NOTICE OF DATA BREACH

To our present and former USA employees:

We regret to inform you that certain personal information of yours may have been obtained by unauthorized third parties.

What happened: Yesterday afternoon, February 26, 2018, our Director of Human Resources received an e-mail from what appeared to be our Global Chief Executive Officer, requesting certain payroll information and copies of 2017 W2s for all of our employees located in the United States. Since this appeared to be a legitimate internal inquiry, our Director of Human Resources responded with a schedule setting forth the requested information and copies of 2017 W2s. Subsequently, we learned that this was not a legitimate internal inquiry, and that this information had been sent to an unknown hacker.

What information was involved: Names, addresses, Social Security numbers, and W2s of all present USA employees and a number of former USA employees. The information did not include dates of birth or driver's license numbers nor did it include spouse/partner or dependents data.

What we are doing: We are reporting this theft to our local police department (Anaheim) and to the Federal Bureau of Investigation (FBI). We are also in the process of notifying the three major credit reporting agencies. We are now actively researching credit monitoring services and will share back with everyone what we can make available in the next few days. We will also schedule a number of Q&A calls for staff to participate in on Thursday, Friday this week and Monday next week. Details will follow very shortly.

What you can do: We recommend that you immediately place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

Equifax: ***equifax.com*** or 1-800-525-6285

Experian: ***experian.com*** or 1-888-397-3742

TransUnion: ***transunion.com*** or 1-800-680-7289

Other Important Information:

You should request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should file a police report. Get a copy of the police report; you may need it to clear up any fraudulent debts.

If your personal information has been misused, visit the FTC's site at ***IdentityTheft.gov*** to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means a potential creditor cannot get your credit report unless you specifically authorize it to do so. That makes it less likely that an identify thief can open new accounts in your name. The cost to place and lift a freeze depends on State law in each State in which you reside. In California, the fee for placing a security freeze on a credit report is \$10 (no fee for residents 65 years of age or older) and we will reimburse you for this cost. If you are a victim of identity theft and submit a valid investigative or incident report, complaint with a law enforcement agency or the Department of Motor Vehicles, the fee will also be waived.

Here is a link to a PDF of *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft:

***[www.bulkorder.ftc.gov/system/files/publications/pdf-0009\\_identitytheft\\_a\\_recovery\\_plan.pdf](http://www.bulkorder.ftc.gov/system/files/publications/pdf-0009_identitytheft_a_recovery_plan.pdf)***

Please also go to the *IdentityTheft.gov* site mentioned above for information about how to report identify theft and steps you can take to help protect yourself from identity theft, depending on the type of information exposed.

For More Information: You may call Annaliesa Chapman, Vice President of Human Resources, at 1-714-385-4965 or e-mail [annaliesa.chapman@ttc.com](mailto:annaliesa.chapman@ttc.com) or [HRUSA@ttc.com](mailto:HRUSA@ttc.com).

I sincerely apologize to you all for this unfortunate incident. Please be assured that the TTC team are diligently working to take steps to ensure this never happens again.



Richard Launder  
President