IDEO·ORG

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

November 9, 2016

Dear Attorney General Foster:

Pursuant to R,S,A. 359-C:20, I(b) we are writing to notify you of a breach of security involving 1 New Hampshire resident.

On September 30, 2016, a work laptop was stolen from an employee's home. The laptop contained personal information that included social security numbers, driver's license numbers, and passport numbers.

The stolen laptop was password protected, and we cannot confirm that the information on the laptop was accessed. We have activated a remote erasure feature that will erase all data stored on the laptop upon connection to the Internet.

The laptop stored the personal information of 1 New Hampshire resident. The affected resident will receive written notification of the security breach by mail on or about November 18, 2016. The affected New Hampshire resident will be offered free credit monitoring, public record monitoring, and identity theft resolution services for 12 months.

We are also investing in additional safeguards to further protect personally identifiable information going forward. Over the next month, we will be rolling out additional password and file protection services across all of IDEO.org. These will provide an additional layer of security around these types of documents and other sensitive information that flows through IDEO.org

If you have any questions, please do not hesitate to contact me at 616.893.8845 or mtaylor@IDEO.org.

Sincerely Yours,

Matt Taylor

IDEO·ORG

Subject: Notice of Data Breach

November 11, 2016

Dear ,

I'm writing to inform you of a breach of personal information at IDEO.org.

What Happened

On September 30, a work laptop of one of our employees was stolen. The laptop contained human resources documents for many of IDEO.org's current and past employees and contractors.

What Information Was Involved

Human resources documents, such as employment verification forms with personally identifiable information are among those documents that could be accessed through this computer. These documents include social security numbers, dates of birth, driver's license information, passport information, and addresses. They also contain this information for a limited number of past and current employees' dependents and beneficiaries.

What We Are Doing

We take the protection of your information seriously. This laptop was password-protected, and we also initiated a protocol to erase the information on this computer upon connection to the internet. We've been working to identify whether or not sensitive information has been accessed, but unfortunately cannot tell definitively whether or not this is the case. So while we have no reason to believe that this information was accessed, we also have no data that would give us the confidence that it was not accessed.

Further, we are investing in additional safeguards to further protect personally identifiable information going forward. Over the next month, we will be rolling out additional password and file protection services across IDEO.org. These will provide an additional layer of security around these types of documents and other sensitive information that flows through IDEO.org.

In addition, we are also offering you Triple Bureau Credit Monitoring/Triple Bureau Credit Report and public records monitoring* services at no charge. These services provide you with alerts for twenty-four months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. Also, the following public records will be monitored: Change of Address, Court Records and Social Security number trace. These services will be provided by IDT911, a company that specializes in identity theft education and resolution.

To enroll in Credit Monitoring* services at no charge, please log on to https://www.myidmanager.com/promo_code.html and follow the instructions provided. When prompted please provide the following unique code to receive services: <UNIQUE CODE HERE.>

To take advantage of the IDT911 services, or to obtain additional information about these services, please call the IDT911 help line *1-800-405-6108* and supply the fraud specialist with your unique code.

What You Can Do

Beyond signing up for IDT911's service, there are other steps you can consider taking to reduce the likelihood of fraud. These include:

- Remain vigilant for fraud and identity theft by carefully checking your credit reports and financial account statements. You can check your credit reports for free through https://www.annualcreditreport.com/. Checking your reports periodically, on top of those provided

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection and in order to confirm your identity.

by [service provider], can help you identify any problems that need to be addressed (fraud-related or otherwise).

- Placing a freeze on new credit by contacting the three major credit bureaus

Equifax	Experian	TransUnion
PO Box 740241	535 Anton Blvd. Suite 100	PO Box 2000
Atlanta, GA 30374	Costa Mesa, CA 92626	Chester, PA 19016
1-888-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	www.transunion.com

- Further information about fraud alerts, security freezes, and identity theft can be obtained from the Federal Trade Commission.

  Bureau of Consumer Protection
  Federal Trade Commission
  600 Pennsylvania Ave., NW
  Washington, DC 20580
  https://www.consumer.ftc.gov
  1-877-438-4338

- Filing your taxes early in the new year. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job.

For More Information

We sincerely apologize for this situation, and we assure you that the safekeeping of your personal information is of the utmost importance to us. Should you have any additional questions regarding this breach, you can call the IDT911 help line at *1-800-405-6108.* You should also feel free to contact me directly at 616-893-8845 or mtaylor@ideo.org if you have any additional questions or concerns.

Matt Taylor