THE TOBIN PROJECT

April 12, 2021

One Mifflin Place, Suite 240
Cambridge, MA 02138

By Mail

Office of the New Hampshire Attorney General
33 Capital Street
Concord, NH 03301

To the Office of the Attorney General:

I am writing to notify you that a breach of security affecting the personal information of one (1) New Hampshire resident was experienced by the Tobin Project, a 501(c)(3) nonprofit organization located at One Mifflin Place, Suite 240, Cambridge, MA 02138.

The Tobin Project became aware on March 21, 2021 of an incident in which a Tobin Project laptop in an employee's possession was stolen. An email account accessible on the laptop contained HR information relating to a small number of current and former Tobin Project fellows, employees, contractors, and affiliates, including the Social Security number of one New Hampshire resident. The Tobin Project began investigating the incident as soon as we became aware of the potential breach, and law enforcement was promptly notified.

The Tobin Project is conducting a thorough review of the potentially affected records; implementing additional security measures, internal controls, and safeguards; and making changes to our policies and procedures to prevent a similar occurrence in the future.

The Tobin Project has no evidence that any of this information was accessed or misused, but we notified the affected individuals on April 12, 2021 out of an abundance of caution. A template copy of the notification sent to the affected New Hampshire resident is enclosed, and the individual has been provided with a code and instructions to sign up for twelve (12) months of credit monitoring services provided by IDX.

For any questions regarding this incident, please contact me at 617-547-2600 or ejoseph@tobinproject.org.

Sincerely,

Euriphile Joseph
Director of Strategy and Operations
The Tobin Project

THE
TOBIN PROJECT

April 12, 2021

NOTICE OF DATA BREACH

One Mifflin Place, Suite 240
Cambridge, MA 02138

Name
Address
City, State Zip

Dear [Name]:

We wanted to notify you of a data security incident involving your Social Security number. The privacy and protection of our employees' and affiliates' information is a matter we take very seriously, and we have worked swiftly to resolve the incident. The Tobin Project deeply regrets the inconvenience this may cause, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What Happened

We became aware on March 21, 2021 of an incident in which a Tobin Project laptop in an employee's possession was stolen. An email account accessible on the laptop contained HR information relating to a small number of current and former Tobin Project fellows, employees, contractors, and affiliates. We began investigating the incident as soon as we became aware of the potential breach, and law enforcement was promptly notified. While we have no evidence that any of this information was accessed or misused, we are providing this notification out of an abundance of caution.

What Information Was Involved

Though the investigation is still underway, we have determined that the information involved in this incident primarily included Social Security numbers.

What We Are Doing

We are conducting a thorough review of the potentially affected records, and are implementing additional security measures, internal controls, and safeguards, and we are making changes to our policies and procedures to prevent a similar occurrence in the future.

We are providing free identity theft prevention and mitigation services from IDX, including credit monitoring and ID theft recovery services for one year, to any individual whose information was exposed by the incident. For details of these services, and to enroll, please visit https://app.idx.us/account-creation/protect or call 1-800-939-4170 and use the enrollment code [XXX]. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note that the deadline to enroll is December 1, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

For More Information

If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us by phone (617-547-2600), by email (ejoseph@tobinproject.org), or by mail at:

The Tobin Project
1 Mifflin Place, Suite 240
Cambridge, MA 02138

Again, we apologize for any inconvenience caused by this incident.

Sincerely,

_____

Euriphile Joseph
Director of Strategy and Operations

What You Can Do

Change Your Passwords

If the information affected included your user name or email address and password or security question and answer for an online account, you should promptly change those account settings or take other appropriate steps to protect that account. You should also take steps appropriate to protect all online accounts which use the same user name or email address and password or security question and answer. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions.

Monitor Your Accounts

You should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps, among others: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Reports

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may

also contact any of the three major consumer reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit File

In addition, you may obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last one year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
(888) 298-0045	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com