



June 13, 2017

**DELIVERED VIA OVERNIGHT MAIL AND EMAIL AT
ATTORNEYGENERAL@DOJ.NH.GOV AND DOJ-CPB@DOJ.NH.GOV**

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear General MacDonald:

Pursuant to N.H. Rev. Stat. Ann. § 359-C: 19 *et seq.*, I am writing to notify you that Intuit Inc. (“Intuit”) recently discovered security incidents involving unauthorized access to some of our customers’ information as a result of fraudulent account log-ins. Between February 3, 2017 and April 11, 2017, Intuit determined that the separate instances of unauthorized access collectively affected two New Hampshire customers of Intuit’s TurboTax business.

Promptly after discovering the issue, we conducted an investigation and took steps to secure our customers’ accounts and information. We determined that an unauthorized party or parties may have accessed these customers’ accounts approximately February 3, 2017 and April 11, 2017, by using legitimate log-in credentials obtained from non-Intuit sources. After accessing the accounts, the unauthorized party or parties may have obtained information contained in a prior year’s tax return or current tax return in progress, such as name, Social Security number, address, date of birth, driver’s license number and financial information (e.g., salary and deductions), and information of other individuals contained in the tax return.

We do not believe this issue resulted from a compromise of credentials from Intuit’s systems. Intuit was not the source of the log-in credentials that were used to gain unauthorized access to the customers’ accounts. Rather, an unauthorized party or parties used log-in credentials stolen from other sources to try to access our customers’ accounts. We have notified the IRS.

One of our top priorities is to help ensure the privacy and security of our customers’ information. Toward that end, we are offering identity protection and credit monitoring services to the affected customers free of charge for one year. Attached for your reference is a sample of the notice to the affected individuals, which we are sending as expeditiously as possible via first class mail.

If you have any questions, please contact me at (650) 944-5136 or Barbara.Lawler@intuit.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Barbara Lawler".

Barbara Lawler
Chief Privacy Officer

Enclosure

CUSTOMER NOTICE TEMPLATE



[Insert date]

Dear **[Insert Recipient Name]**:

We are writing to notify you that, during a security review on **[insert date]**, we determined that your TurboTax account may have been accessed by an unauthorized party. Promptly after discovering the issue, we conducted an investigation and took steps to secure your account.

Based on our investigation, it appears an unauthorized party may have accessed your account by using your username and password combination that was obtained from a non-Intuit source. The unauthorized access occurred **[on/from] [date/date range]**. By accessing your account, the unauthorized party may have obtained information contained in a prior year's tax return or your current tax return in progress, such as your name, Social Security number, address(es), date of birth, driver's license number and financial information (e.g., salary and deductions), and information of other individuals contained in the tax return.

We deeply regret that this incident may affect you. Intuit has taken various measures to help ensure that the accounts of affected customers are protected. We are notifying you so you can take steps to help protect your information.

How we're protecting your account:

We've made your TurboTax account temporarily unavailable to protect your information from further unauthorized access. To help protect you, we're offering you one year of free identity protection, credit monitoring and identity restoration services through Experian IdentityWorksSM, provided by our credit-monitoring partner Experian. The Reference Guide included with this letter provides details on how to use this service. If information about a spouse or dependents appears on your tax return, please email us at TTaxInvestigations@intuit.com to obtain credit monitoring services for these individuals.

Your next steps:

1. To reactivate your account or for other assistance, please call Customer Care at 1-800-944-8596 and say the word "Security" at the prompt, or email us at TTaxInvestigations@intuit.com.
2. We will walk you through the process of verifying your identity so you may access your account.
3. Once you access your account, please review your personal information in MyTurboTax to make sure that it is accurate. Pay particular attention to your email address and bank account information. To further protect your information, you can use the Google Authenticator app for verification upon every login. Just click the two-step verification option on the Account Settings page to enable this feature or for more information.

4. To prevent unauthorized access to your non-Intuit online accounts, we recommend that you immediately change your passwords for those accounts, particularly if you use the same username and password as the one used for your Intuit online account.
5. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by monitoring your free credit reports and reviewing your account statements. The attached Reference Guide provides additional details to help you protect your personal information.

We sincerely regret any inconvenience this may cause you. If you have any additional questions or concerns, please call our security hotline at [1-800-944-8596](tel:1-800-944-8596).

Sincerely,

A handwritten signature in black ink, appearing to read "Barbara Lawler". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Barbara Lawler
Chief Privacy Officer

Reference Guide

We encourage you to take the following steps:

Enroll in Identity Protection and Credit Monitoring Services; Access Identity Restoration Services if Needed.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one-year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** [\[date\]](#) (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [\[URL\]](#)
- Provide your **activation code:** [\[code\]](#)

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by [\[enrollment end date\]](#). Be prepared to provide engagement number [\[engagement number\]](#) as proof of eligibility for the Identity Restoration services by Experian.

Additional details regarding your 12-Month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*

- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** 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

What else you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information, and refer to the additional steps below.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission’s (“FTC”) website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the “inquiries” section for names of creditors from whom you haven’t requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the “personal information” section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can’t be explained, then you will need to call the creditors involved. Information that can’t be explained also should be reported to your local police or sheriff’s office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity

theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Place an initial fraud alert.
- Order your credit reports.
- Create an FTC Identity Theft Affidavit by submitting a report about the theft at <http://www.ftc.gov/complaint> or by calling the FTC.
- File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report.
- Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from furnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting agencies, and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
 Consumer Response Center
 600 Pennsylvania Avenue, NW
 Washington, DC 20580
 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

| | | | |
|----------|---|----------------|--|
| Equifax | Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374 | 1-800-525-6285 | www.equifax.com |
| Experian | Experian Inc. P.O. Box 9554 Allen, TX 75013 | 1-888-397-3742 | www.experian.com |

| | | | |
|------------|---|----------------|--------------------|
| TransUnion | TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 | 1-800-680-7289 | www.transunion.com |
|------------|---|----------------|--------------------|

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or

remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov