Intuit
2535 Garcia Avenue
Mountain View, CA 94043

STATE OF NH
DEPT OF JUSTICE
2017 FEB -2 AM 9:47

intuit

February 1, 2017

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

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

Dear General Foster:

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. On January 20, 2017, Intuit determined that the separate instances of unauthorized access collectively affected one New Hampshire customer 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 this customer's account on approximately January 20, 2017, by using legitimate log-in credentials obtained from non-Intuit sources. After accessing the account, 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 customer free of charge for one year. Attached for your reference is a sample of the notice to the affected individual, 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,

Barbara Lawler
Chief Privacy Officer

Enclosure

CUSTOMER NOTICE TEMPLATE

Intuit
7535 Torrey Santa Fe Road
San Diego, CA 92129

STATE OF IOWA
OFFICE OF THE ATTORNEY GENERAL
2017 FEB -2 AM 9:47

intuit

Date

Dear [Recipient Name]:

We are committed to the security of our customers' information and make every effort to inform you of security concerns that may affect you as quickly as possible. We are contacting you because, during a security review on [blank date] we concluded that your TurboTax account may have been accessed on a previous date by someone other than you.

If your account was accessed by someone other than you, we believe your username and password combination was obtained from a non-Intuit data breach, phishing email, or compromised website. The unauthorized access occurred on [date range]. Based on our analysis, this means that someone else may have obtained information contained in a prior year 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, deductions); including the information of any other person(s) listed in a prior and/or current year tax return.

Intuit has taken a variety of measures to ensure that the accounts of affected customers are protected. We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm.

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 in the future, we're offering you free credit monitoring through ProtectMyID service, provided by our credit-monitoring partner Experian. The information included with this letter provides details about how to use this service. Feel free to email us at TTaxInvestigations@intuit.com with questions about how to obtain credit-monitoring service if you have a spouse or dependents that appear on your return.

Your next steps:

1. To reactivate your account, please call Customer Care at 1-800-944-8596 or email us at TTaxInvestigations@intuit.com.
2. We'll walk you through the process of verifying your identity so you may access your account again.
3. Once you access your account, review your personal information in MyTurboTax to make sure that it's accurate. Pay particular attention to your email address and bank account information. To further protect yourself, 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 if you would like more information.
4. To prevent unauthorized access to your other non-Intuit online accounts, you should immediately change your passwords for those accounts, particularly if you use the same username and password.

5. Make sure that your computer is properly secured (e.g., that you are using current anti-virus software, firewall, security patches) and you routinely check for viruses and malware. More information on how to do this can be found at https://security.intuit.com/protect-your-computer.html
6. Because this is a serious incident, we strongly encourage you to take preventive measures now to help prevent and detect any misuse of your information:
    a. As a first preventive step, we recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. We also suggest you submit a complaint with the Federal Trade Commission, located at 600 Pennsylvania Avenue NW, Washington, DC 20580, by calling 1-877-ID-THEFT (1-877-438-4338) or visiting their website online at https://www.ftccomplaintassistant.gov/. Submitting a report of suspected incidents regarding your personal information to local law enforcement or your State Attorney General can also help address incidents of identity theft.
    b. As a second step, you also may want to contact the three U.S. credit reporting agencies (Equifax, Experian and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com.
    c. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. A victim's personal information is sometimes retained for use at a later time. Checking your credit reports periodically may help you spot problems and address them quickly. Remaining vigilant about reviewing account statements and monitoring free credit reports is extremely important in the effort to protect your information from incidents of fraud and identity theft.
    d. To protect yourself from the possibility of identity theft, some state laws allow you to place a security freeze on your credit files. By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three U.S. credit reporting agencies to place the security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than $10 for each credit reporting agency for a total of $30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

To obtain a security freeze, contact the following agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-888-298-0045
https://www.freeze.equifax.com/

TransUnion
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
https://freeze.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze

In addition to information about security freezes, these credit monitoring agencies can also provide you with information about fraud alerts.

For More Information
For more information on identity theft, we suggest that you visit the web site of the California Office of Privacy Protection at http://oag.ca.gov/idtheft.

If you have any additional questions or concerns, please call our security hotline at 1-800-944-8596.

Sincerely,

Barbara Lawler, Chief Privacy Officer, Intuit

Activate ProtectMyID Now in Three Easy Steps

1. **Enroll by <insert date>.** Your code will not work after this date.
2. **Visit the ProtectMyID Web Site to enroll:** www.protectmyid.com/protect
3. **Provide your activation code:** <insert code(s)>

If you have questions or need an alternative to enrolling online, please call 866-751-1324 and provide engagement number: **# <insert engagement number>**.

Additional Details Regarding Your 12-Month ProtectMyID Membership

- You do not need a credit card to enroll.
- Once your ProtectMyID membership is activated, you will receive the following features:
  - **Free copy of your Experian credit report**
  - **Surveillance alerts for:**
    - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian credit report.
  - **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
    - Identity theft can happen months and even years after personal information has been obtained. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of fraud resolution support even after your ProtectMyID membership has expired.
  - **$1 Million Identity Theft Insurance*:** Immediately covers certain costs, including lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-297-7780.

What you can do to protect your information: Please refer to the last page of this letter to see additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s).

---

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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

Additional Actions to Help Reduce Your Chances of Identity Theft

- **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**
  An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance. These credit monitoring agencies can also provide you with information about fraud alerts.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**
  If you are concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when applying for any type of credit. This process is also completed through each of the credit reporting companies. The cost of placing the freeze is no more than $10 for each credit reporting agency for a total of $30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the FTC, there may be no charge to place the freeze.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**
  Visit www.annualcreditreport.com or call 877-322-8228.
  Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **MANAGE YOUR PERSONAL INFORMATION**
  Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

- **USE TOOLS FROM CREDIT PROVIDERS**
  Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. A victim's personal information is sometimes retained for use at a later time. Checking your credit reports periodically may help you spot problems and address them quickly. Remaining vigilant about reviewing account statements and monitoring free credit reports is extremely important in the effort to protect your information from incidents of fraud

and identity theft. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**
  - Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html.
  - The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically.
  - Your State Attorney General's Office has information about steps you can take to avoid identity theft. Submitting a report of suspected incidents regarding your personal information to local law enforcement or your State Attorney General can also help address incidents of identity theft.
    - North Carolina Residents: Contact the North Carolina Attorney General's Office at ncdoj.gov/Consumer.aspx, 1-877-566-7226, or 9001 Mail Service Center, Raleigh, NC 27699-9001.
    - Maryland Residents: Contact the Maryland Office of the Attorney General at http://www.oag.state.md.us/idtheft/index.htm, 410-576-6491, idtheft@oag.state.md.us, or 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.