

[REDACTED]



February 11, 2015

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord NH 03301

RE: Notification of security incident involving Intuit customers

Sent via email to: DOJ-CPB@doj.nh.gov

Dear Sir or Madam,

In accordance with state law, I am writing to inform you about a security incident involving customers of our TurboTax service. We discovered on January 30, 2015 that unknown individual(s) have accessed customer accounts during the timeframe of April 2014 and September 2014. These individuals used legitimate credentials (userid and password) obtained elsewhere to view customer tax returns. These tax returns contained –personal information including name, postal address, social security number and financial information.

Upon learning of this exposure we immediately took steps to investigate, secure the account, and inform the IRS. We are continuing to work with the IRS and FBI as they investigate this incident. We have also informed the appropriate state revenue authorities. We are confident that our systems remain secure and that this incident occurred through use of credentials that the perpetrators obtained elsewhere.

We take the privacy and security of our customer data very seriously. We are continuing to support law enforcement agencies in their investigation and are making contact with the 33 impacted customers in your state to provide notice. The notice will describe, among other things (1) the general nature of the incident (2) the type of personal information that was exposed, (3) precautionary measures we took for their account (4) contact information for inquiries and (5) how to enroll in identity theft restoration and continuous credit monitoring services, which are being made available by Intuit for affected individuals free of charge.

Please feel free to contact me if you require any additional information concerning this matter.

Sincerely,

Thomas Hale

[REDACTED]



February 5, 2015

Dear <insert Name(s)>:

We've identified what appears to be unauthorized access to your TurboTax account on or around January 29, 2015. As a result, criminals may have obtained information contained on your prior year tax returns. This letter details steps we've taken to help protect you and suggestions on how to protect yourself in the future. Please feel free to call us if you have questions. We are here to help.

We have no way of knowing who did this or how they obtained your login credentials, but our investigation confirmed that the username and password they used to login were **not** obtained from any Intuit system. Unfortunately, criminals gain access to legitimate username and password combinations from many different sources, including from security breaches elsewhere. We recommend you check your computer for malware or viruses immediately. Your security and privacy are very important to us. We've taken action to address this situation, including locking your TurboTax account to prevent further unauthorized access and working with federal law enforcement agencies to try to locate the criminals who accessed your account.

How we're protecting your account

We've locked your TurboTax account to protect your information from further unauthorized access. To help ensure you're protected 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 unlock your account, please email us at TTaxInvestigations@intuit.com or call Customer Care at **866-602-4279**. We'll tell you how to change your login information and access your account again.
2. Once you access your account, review your personal information in MyTurboTax to make sure that it's accurate. Make sure to review your email address and bank account information.
3. 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 as you use with TurboTax.
4. Make sure that your computer is properly secured (e.g., anti-virus software, firewall, security patches). More information on how to do this can be found at <https://security.intuit.com/protect-your-computer.html>.

Please let me know if you have any additional questions or concerns.

Sincerely,

Bob Meighan, Vice President, Customer Advocacy, turbotax_advocate@intuit.com

Activate ProtectMyID Now in Three Easy Steps

1. **Enroll by April 30, 2015.** Your code will not work after this date.
2. **Visit the ProtectMyID Web Site to enroll:** www.protectmyid.com/alert
3. **Provide your activation code:** <insert code(s)>

If you have questions or need an alternative to enrolling online, please call 877-297-7780 and provide engagement number: PC89766

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 a data breach. 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 are 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 take 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.

Equifax

1-800-525-6285

www.equifax.com

Experian

1-888-397-3742

www.experian.com

TransUnion

1-800-680-7289

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.

➤ 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. 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> for general information regarding protecting your identity.

- 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.