162 3063

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Maureen K. Ohlhausen, Acting Chairman**
Terrell McSweeny

In the Matter of **TAXSLAYER, LLC, a limited liability company.**	**DOCKET NO. C-4626**

COMPLAINT

The Federal Trade Commission, having reason to believe that TaxSlayer, LLC, a limited liability company, ("TaxSlayer" or "Respondent"), has violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a); the Privacy of Consumer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313, recodified at 12 C.F.R. § 1016 ("Reg. P"), and issued pursuant to Sections 501-504 of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. §§ 6801-6803; and the Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Sections 501(b) and 505(b)(2) of the GLB Act, 15 U.S.C. §§ 6801(b), 6805(b)(2);2(o)5(S)12(22uT S)1(t)-ax,nancnge7sued

5.

a. Designating one or more employees to coordinate the information security program;

b. Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks;

c. Designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures;

d. Overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and

e. Evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

15. Respondent violated the Safeguards Rule. For example:

a. Respondent failed to have a written information security program until November 2015.

b. Respondent failed to conduct a risk assessment, which would have identified reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, including risks associated with inadequate authentication.

c. Respondent failed to implement information safeguards to control the risks to customer information from inadequate authentication. For example:

i. Respondent did not require consumers to choose strong passwords when setting up their accounts, which is a standard practice for accounts containing sensitive personal information. Respondent's only requirement for passwords was that they be eight to sixteen characters in length. This created a risk that attackers could guess commonly-used passwords, or use dictionary attacks, to access TaxSlayer Online accounts.

ii. Respondent failed to implement adequate risk-based authentication measures sufficient to mitigate the risk of list validation attacks when such attacks became reasonably foreseeable. List validation attacks occur when remote attackers use lists of stolen login credentials to attempt to access accounts across a number of popular Internet sites, knowing that consumers often reuse user name and passwords combinations.

iii. Respondent failed to inform TaxSlayer Online users when a material change was made to the mailing address, password, or security question associated with their accounts. Respondent also failed to inform TaxSlayer Online users when a material change is made to the bank account routing number or the payment method for a refund (e.g., from bank account to a pre-paid debit card) associated with their accounts.

iv. Respondent failed to require customers to validate their email addresses at account creation, in order to verify accuracy and communicate with customers regarding security-related issues.

v. Respondent failed to use readily-available tools to prevent devices or IP addresses from attempting to access an unlimited number of TaxSlayer Online accounts in rapid succession through a list validation attack.

16. Respondent became subject to a list validation attack that began on October 10, 2015, and ended on December 21, 2015. On that day, Respondent implemented multi-factor authentication, requiring users to first submit their username and password, and then to authenticate their device by, for example, entering a code that Respondent sent to the user's email or mobile phone.

17. As part of this list validation attack, the remote attackers were able to gain full access to 8,882 existing TaxSlayer Online accounts. In an unknown number of instances, the attackers engaged in tax identity theft by altering the bank routing and refund methods, e-filing fraudulent tax returns, and diverting the fabricated tax refunds to themselves. Customers were not notified when these alterations occurred. Respondent was not aware of this list validation attack until a TaxSlayer Online user called on January 11, 2016 to report suspicious activity on her account.

18. Consumers who are the victims of tax identity theft spend significant time resolving this problem. Victims spend time calling the IRS and state tax authorities to report the tax identity theft. Victims then have to obtain PIN numbers from the IRS and file their taxes on paper using those PIN numbers. They then have to wait months to receive their tax refunds. To protect themselves and their dependents from future identity theft, victims freeze or place holds on their credit, and they spend additional time monitoring their credit histories and financial accounts. These victims also suffer out-of-pocket financial losses.

Count I
Violations of the Privacy Rule and Reg. P

19. As described in Paragraphs 11 to 13, the Privacy Rule and Reg. P require financial institutions to provide customers with a clear and conspicuous privacy notice that accurately reflects the financial institution's privacy policies and practices. Further, financial institutions must deliver the privacy notice so that each customer could reasonably be expected to receive actual notice.

20. Respondent is a financial institution, as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).

21. As set forth in Paragraph 13.a

30. Pursuant to the GLB Act, violations of the Safeguards Rule and the Privacy Rule are enforced through the FTC Act.

THEREFORE, the Federal Trade Commission this twentieth day of October, 2017, has issued this Complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL: