1623063

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-**

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); and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent is a Georgia limited liability corporation with its principal office at 3003 TaxSlayer Drive, Evans, Georgia 30809.

2. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent advertises, offers for sale, sells, and distributes products and services to consumers, including TaxSlayer Online, a tax return preparation and electronic filing software and service.

4. Respondent is a business that began more than 50 years ago as a tax return preparation firm. It developed tax return preparation software for its internal use in the 1980s. In the 1990s, it developed a browser-based software service that it advertises, offers for sale, sells, and distributes to assist consumers in preparing and electronically filing federal and state income tax returns. Over the years, Respondent added other tax return preparation products, including a mobile app. This Complaint refers to the browser-based software service and mobile app as "TaxSlayer Online."

5. In 2016, more than 950,000 individuals filed tax returns with TaxSlayer Online.

6. Respondent typically charges consumers fees for the use of TaxSlayer Online.

7. TaxSlayer Online users create an account by entering a username and password ("login credentials") on an account creation page.

8. They then input a host of personal information in order to create a tax return, including but not limited to: name, Social Security number ("SSN"), telephone number, physical address, income, employment status, marital status, identity of dependents, financial assets, financial activities, receipt of government benefits, home ownership, indebtedness, health insurance, retirement information, charitable donations, tax payments, tax refunds, bank account numbers, and payment card numbers. Respondent also collects IP addresses and persistent identifiers associated with the particular device from which the tax return is prepared and/or filed.

9. TaxSlayer Online uses this personal information to prepare tax returns on behalf of customers. Once a tax return is prepared, a customer can file the return electronically through TaxSlayer Online with the Internal Revenue Service ("IRS") and state departments of revenue. If a customer is entitled to a refund, Respondent offers the option of transferring the refund directly into a customer's bank account. Customers may also elect to receive their tax refunds on a prepaid debit card.

RESPONDENT'S GRAMM-LEACH-BLILEY ACT ("GLB ACT") VIOLATIONS

10. Respondent is a financial institution subject to the GLB Act, as that term is defined by Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A), because among other things, Respondent provides tax planning and tax preparation services, 16 C.F.R. § 313.3(k)(2)(viii); 12 C.F.R. § 1016.3(l)(3)(ii)(H); 12 C.F.R. § 225.28(b)(6)(vi) ("Reg. Y"), and data processing, 12 C.F.R. § 225.28(b)(14). Respondent collects nonpublic personal information, as defined by 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1)-(3). Because Respondent is a financial institution that collects nonpublic personal information, it is subject to the requirements of the GLB Privacy Rule, 16 C.F.R. Part 313, Reg. P., 12 C.F.R. Part 1016, and the Safeguards Rule, 16 C.F.R. Part 314.

Privacy Rule and Reg. P

11. The Privacy Rule, which implements Sections 501-503 of the GLB Act, 15 U.S.C. §§ 6801-6803, was promulgated by the Federal Trade Commission on May 24, 2000, and became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule, and accordingly promulgated the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. Part 1016 ("Reg. P"), which became effective on October 28, 2014. Accordingly, Respondent's conduct is governed by the Privacy Rule prior to October 28,

2014, and by Reg. P after that date. The GLB Act authorizes both the CFPB and the Federal Trade Commission to enforce Reg. P. 15 U.S.C. § 6805.

12. Both the Privacy Rule and Reg. P require financial institutions to provide consumers with an initial and annual privacy notice. Both the initial and annual privacy notices must be "clear and conspicuous," 16 C.F.R. § 313.3(b) and 12 C.F.R. § 1016.3(b), and must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. §§ 313.4 and 313.5 and 12 C.F.R. §§ 1016.4 and 1016.5. The privacy notice must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the security and confidentiality policies of the financial institution. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. A financial institution must provide its privacy notice so that each consumer can reasonably be expected to receive actual notice. 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. An example, for the consumer who conducts transactions electronically, is to require the consumer to acknowledge receipt of the initial notice as a necessary step to obtaining the financial product or service. 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9; Privacy of Consumer Financial Information, 65 Fed. Reg. 33646-01, at 33665-66 (May 24, 2000).

13. Respondent failed to comply with the Privacy Rule requirements discussed in Paragraph 12. Specifically:

    a. Respondent failed to provide a clear and conspicuous initial privacy notice. 16 C.F.R. § 313.4, 12 C.F.R. § 1016.4. Respondent's Privacy Policy was contained towards the end of a long License Agreement, and Respondent did not convey the importance, nature, and relevance of this Privacy Policy to its customers.

    b. Respondent failed to deliver the initial privacy notice so that each customer could reasonably be expected to receive actual notice. 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. For example, Respondent did not require customers to acknowledge receipt of the initial notice as a necessary step to obtaining a particular financial product or service.

Safeguards Rule

14. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003. The Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing, implementing, and maintaining a comprehensive information security program that is written in one or more readily accessible parts, and that contains administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue, including:

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, Respondent failed to provide its customers with a clear and conspicuous initial privacy notice. Therefore, Respondent violated the Privacy Rule, 16 C.F.R. § 313.4, and Reg. P, 12 C.F.R. § 1016.4.

22. As set forth in Paragraph 13.b, Respondent failed to deliver the initial privacy notice so that each customer could reasonably be expected to receive actual notice. Therefore, Respondent violated the Privacy Rule, 16 C.F.R. § 313.9; and Reg. P., 12 C.F.R. § 1016.9.

23. Therefore, the conduct set forth in Paragraphs 21 and 22 is a violation of the Privacy Rule and Reg. P.

Count II
Violations of the Safeguards Rule

24. As described in Paragraph 14, the Safeguards Rule requires financial institutions to have a written comprehensive information security program that include specified elements, including a requirement to conduct a risk assessment. It also requires financial institutions to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and then design and implement information safeguards to control the risks identified through the risk assessment.

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

26. As set forth in Paragraph 15a, Respondent failed to have a written comprehensive information security program until November 2015.

27. As set forth in Paragraph 15b, Respondent did not conduct risk assessments to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

28. As set forth in Paragraph 15c, Respondent did not implement information safeguards to control risks, specifically the risk that remote attackers were using stolen account credentials to take over customers' TaxSlayer Online accounts in order to perpetrate tax identity theft.

29. Therefore, the conduct set forth in Paragraphs 26 to 28 is a violation of the Safeguards Rule.

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 _____ day of _____, 2017, has issued this Complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL: