

Complaint

IN THE MATTER OF

TAXSLAYER, LLCCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT, THE
GRAMM-LEACH-BLILEY ACT PRIVACY RULE AND SAFEGUARDS
RULE, AND REGULATION P*Docket No. C-4626; File No. 162 3063**Complaint, October 20, 2017 – Decision, October 20, 2017*

This consent order addresses TaxSlayer, LLC's products and services, including TaxSlayer Online, a browser-based tax return preparation and electronic filing software and service. The complaint alleges that TaxSlayer failed to comply with the Gramm-Leach-Bliley ("GLB") Act Privacy Rule. The complaint further alleges that TaxSlayer engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive information from consumers, in violation of the GLB Act Safeguards Rule. The consent order prohibits TaxSlayer from violating any provision of the GLB Act Privacy Rule and Safeguards Rule and requires TaxSlayer to obtain an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part I.B of the order, and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of sensitive consumer information has been protected.

Participants

For the *Commission*: *Jacqueline K. Connor* and *Katherine E. McCarron*.

For the *Respondent*: *Bilal K. Sayyed, McDermott Will & Emery*.

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

Complaint

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.

Complaint

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

Complaint

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

Complaint

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;

Complaint

- 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,

Complaint

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.

Complaint

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.

Complaint

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 twentieth day of October, 2017, has issued this Complaint against Respondent.

Decision and Order

By the Commission.

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violation of the Federal Trade Commission’s Privacy of Consumer Financial Information Rule (“Privacy Rule”), 16 C.F.R. Part 313, recodified at 12 C.F.R. § 1016 (“Regulation P”), and the Federal Trade Commission’s Standards for Safeguarding Customer Information Rule (“Safeguards Rule”), 16 C.F.R. Part 314, each issued pursuant to Title I of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and Section 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, the Privacy Rule, Regulation P, and the Safeguards Rule, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. Now, in further conformity with the procedure described in

Decision and Order

Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent, TaxSlayer, LLC, is a Georgia limited liability corporation with its principal office at 3003 TaxSlayer Drive, Evans, Georgia 30809.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. “Personal information” means individually identifiable information from or about an individual consumer, including but not limited to: (1) email address; (2) user account credentials, such as a login name and password; (3) first and last name; (4) government-issued identification number, such as a Social Security number; (5) mobile or other telephone number; (6) home or other physical address, including street name and name of city or town; or (7) any information from or about an individual consumer that is combined with any of (1) through (6) above.
- B. “Covered product or service” means any tax return preparation product or e-filing service, including any plan or program.
- C. “Respondent” means TaxSlayer, LLC, and its successors and assigns.

Decision and Order

Provisions**I. GLB Rule Violations**

IT IS ORDERED that Respondent, and Respondent's officers, agents, employees and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from violating any provision of:

- A. The Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313, or the Privacy of Consumer Financial Information Rule (Regulation P), 12 C.F.R. Part 1016; or
- B. The Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314.

In the event that any of the statutory sections or rules identified in this Part are hereafter amended or modified, compliance with that statutory section or rule as so amended or modified shall not be a violation of this Order.

II. Biennial Assessment Requirements

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, in connection with their compliance with Section I (A) and (B) of this Order, shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the Order for the initial Assessment, and (2) each two-year period thereafter for ten (10) years after service of this Order for the biennial Assessments. Each Assessment shall:

- A. Set forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;

Decision and Order

- B. Explain how such safeguards are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. Explain how the safeguards that have been implemented meet or exceed the protections required by Section I (B) of this Order, and
- D. Certify that Respondent's security program(s) is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. The Assessment must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be: an individual qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); an individual holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

Respondent must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must retain all subsequent biennial Assessments, at least until the Order terminates. Respondent must submit any biennial Assessments to the Commission within 10 days of a request from a representative of the Commission.

III. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgements of receipt of this Order:

Decision and Order

- A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 20 years after issuance of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibilities for the conduct specified in Provisions I through IV; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which a Respondent delivered a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

IV. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which:
 - 1. Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (b) identify all of the Respondent's businesses by their names, primary telephone numbers, and primary physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered; (d) describe in detail whether and how

Decision and Order

Respondent is in compliance with each Provision of this Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:
 - 1. Respondent must submit notice of any change in:
 - (a) any designated point of contact; or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,

Decision and Order

Washington, DC 20580. The subject line must begin:
In re TaxSlayer, LLC.

V. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain such records for 5 years. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and, if applicable, the reason for termination;
- C. Records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;
- D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;
- E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security and confidentiality of Personal Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, security and confidentiality of Personal Information;
- F. For 5 years from the date of the last dissemination of any representation covered by this Order:
 - 1. All materials that were relied upon in making the representation; and

Decision and Order

2. All evidence in Respondent's possession, custody, or control that contradicts, qualifies, or otherwise calls into question the representation, or the basis relied upon for the representation, including complaints and other communications with consumers or with governmental or consumer protection organizations; and
- G. For 5 years from the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment.

VI. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of

Decision and Order

identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

VII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on October 20, 2037, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any provision in this Order that terminates in less than 20 years;
- B. This Order's application to a Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision, as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from TaxSlayer, LLC (“TaxSlayer”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received and will decide whether it should withdraw from the agreement or make final the agreement’s proposed order.

This matter involves TaxSlayer, a company that advertises, offers for sale, sells, and distributes products and services to consumers, including TaxSlayer Online, a browser-based tax return preparation and electronic filing software and service. TaxSlayer Online assists consumers, typically for a fee, in preparing and electronically filing federal and state income tax returns. In 2016, more than 950,000 individuals filed tax returns using TaxSlayer Online.

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

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, TaxSlayer offers the option of directing the refund into a

Analysis to Aid Public Comment

customer's bank account, or customers may elect to receive their refunds on a prepaid debit card.

The complaint alleges that TaxSlayer became subject to a list validation attack that began in October 2015. List validation attacks occur when attackers use lists of stolen login credentials to attempt to access accounts across a number of websites, knowing that consumers often reuse login credentials. In an unknown number of instances, the attackers engaged in tax identity theft by e-filing fraudulent tax returns and diverting the fabricated refunds to themselves.

The Commission's complaint alleges that TaxSlayer failed to comply with the Gramm-Leach-Bliley ("GLB") Act Privacy Rule in two ways. First, TaxSlayer failed to provide a clear and conspicuous initial privacy notice. TaxSlayer's Privacy Policy was contained towards the end of a long License Agreement, and TaxSlayer did not convey the importance, nature, and relevance of this Privacy Policy to its customers. Second, TaxSlayer failed to deliver the initial privacy notice so that each customer could reasonably be expected to receive actual notice. For example, TaxSlayer did not require customers to acknowledge receipt of the initial privacy notice as a necessary step to obtaining a particular financial product or service.

In addition, the complaint alleges that TaxSlayer engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive information from consumers, in violation of the GLB Act Safeguards Rule. First, TaxSlayer failed to have a written information security program until November 2015. Second, TaxSlayer failed to conduct a risk assessment, which would have identified reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, including risks associated with inadequate authentication. Third, TaxSlayer failed to implement information safeguards to control the risks to customer information from inadequate authentication.

The proposed order contains provisions designed to prevent TaxSlayer from engaging in practices similar to those alleged in the complaint. Part I prohibits TaxSlayer from violating any provision of the GLB Act Privacy Rule and Safeguards Rule. Part

Analysis to Aid Public Comment

II of the proposed order requires TaxSlayer to obtain, within the first one hundred eighty (180) days after service of the order and on a biennial basis thereafter for a period of ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part I.B of the order, and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of sensitive consumer information has been protected.

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires dissemination of the order now and in the future to all current and future principals, officers, directors, and LLC managers and directors, and to persons with managerial or supervisory responsibilities relating to Parts I through IV of the order. Part IV ensures notification to the FTC of changes in corporate status and mandates that TaxSlayer submit an initial compliance report to the FTC. Part V requires TaxSlayer to retain documents relating to its compliance with the order for a five-year period. Part VI mandates that TaxSlayer make available to the FTC information or subsequent compliance reports, as requested. Part VII is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order, or to modify in any way the proposed order’s terms.

Complaint

IN THE MATTER OF

1-800 CONTACTS, INC.COMPLAINT AND INITIAL DECISION IN REGARD TO ALLEGED
VIOLATIONS OF SECTION 5 OF THE FEDERAL TRADE COMMISSION
ACT*Docket No. 9372; File No. 141 0200**Complaint, August 8, 2016 – Initial Decision, October 27, 2017*

This case addresses 1-800 Contacts, Inc.'s settlement agreements with over a dozen rivals prohibiting both 1-800 and the other parties from bidding on keywords containing the other's trademarks, and requiring each party to implement negative keywords to ensure that their ads do not appear in search engine results pages for searches that contain each other's trademarks. The complaint alleges that these agreements are in restraint of trade in violation of Section 5 of the FTC Act. In his Initial Decision, the Administrative Law Judge found that the Challenged Agreements pose significant, unjustified anticompetitive consequences in the relevant market for the sale of contact lenses online. The Administrative Law Judge ordered 1-800 Contacts to cease and desist from enforcing or attempting to enforce any and all provisions, terms, or requirements in an existing agreement or court order that impose a condition on a Seller, which prohibits, restricts, regulates, or otherwise places any limitation on truthful, non-deceptive, and non-infringing advertising or promotion.

Participants

For the *Commission*: Joshua Barton Gray, Gustav Chiarello, Kathleen Clair, Stuart Hirschfeld, Nathaniel Hopkin and Charlotte Slaiman.

For the *Respondent*: Garth Vincent, Munger Tolles & Olson; Darryl Nirenberg, Steptoe & Johnson.

COMPLAINT

Pursuant to the provisions of the Federal Trade Commission Act, and by virtue of the authority vested in it by said Act, the Federal Trade Commission ("Commission"), having reason to believe that 1-800 Contacts, Inc. ("1-800 Contacts"), a corporation, hereinafter sometimes referred to as "Respondent," has violated the provisions of said Act, and it appearing to the Commission that a proceeding in respect thereof would be in the