

Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of TaxSlayer, LLC, File No. 1623063

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 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 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.