UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Terrell McSweeny

FTC Matter No. P155402

ORDER TO FILE A SPECIAL REPORT

Pursuant to a resolution of the Federal Trade Commission ("FTC" or "the Commission") dated March 4, 2016, titled "Resolution Directing Use of Compulsory Process to Collect Information Regarding Data Security Auditors," copy of which is enclosed, [COMPANY NAME], hereinafter referred to as the "Company," is ordered to file with the Commission, no later than 45 days after date of service, a Special Report containing the information and documents specified herein.

The Commission is seeking insight into data security compliance auditing and its role in protecting consumers' information and privacy. The Special Report will assist the Commission in compiling a study of such auditors and their policies, practices, and procedures.

The Special Report must restate each item of this Order with which the corresponding answer is identified. Your report is required to be subscribed and sworn by an official of the Company who has prepared or supervised the preparation of the report from books, records, correspondence, and other data and material in your possession. If any question cannot be answered fully, give the information that is available and explain in what respects and why the answer is incomplete. The Special Report and all accompanying documentary responses must be Bates-stamped.

Confidential or privileged commercial or financial information will be reported by the Commission on an aggregate or anonymous basis, consistent with Sections 6(f) and 21(d) of the FTC Act. Individual submissions responsive to this Order that are marked "confidential" will not be disclosed without first giving the Company ten (10) days notice of the Commission's intention to do so, except as provided in Sections 6(f) and 21 of the FTC Act.

Specifications

Please provide the following information, documents, and items, consistent with the definitions, instructions, and formatting requirements contained in Attachment A:

1. **Identification of Report Author**: Identify by full name, business address, telephone number, and title of the person(s) who prepared or supervised the preparation of the Company's response to this Order and describe in detail the steps taken by the Company to respond to this Order. For each specification, identify the individual(s) who assisted in preparation of the response. Provide a list of the persons (identified by name and corporate title or job description) whose files were searched and identify the person who conducted the search.

2. **Company Information**:

    a. State the Company's complete legal name and all other names under which it has done business, its corporate mailing address, all addresses from which it does or has done business, and the dates and states of its incorporation.

    b. Describe the Company's corporate structure, and state the names of all parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, websites, and entities over which it exercises supervision or control. For each such entity, describe the nature of its relationship to the Company.

    c. Identify each individual or entity having an ownership interest in the Company, as well as their individual ownership stakes and their positions and responsibilities within the Company.

3. **Products and Services**:

    a. **Payment Card Industry Data Security Standard ("PCI DSS") Compliance Assessments**

        i. State whether the Company performs PCI DSS Compliance Assessments and, if so, describe the nature of the service, the length of time that the Company has been certified to perform PCI DSS Compliance Assessments, the process by which the Company became certified to perform these Assessments, and the number of Compliance Assessments that the company has performed annually for each year of the Applicable Time Period.

ii. For each year of the Applicable Time Period, state the Company's (a) annual total gross revenue; and (b) annual gross revenue attributable to Compliance Assessments.

iii. State whether the Company employs any Qualified Security Assessors ("QSAs") and, if so, state:

    1. the number of QSAs currently employed by the Company;

    2. the qualifications and/or certifications that the Company requires QSAs to obtain;

    3. any additional or recurrent training the Company requires QSAs to undergo, including a description of each training requirement, the names of the companies or individuals providing the training, and the frequency with which each QSA must undergo each training; and

    4. provide copies of all policies and procedures relating to the qualification and training requirements for QSAs, including but not limited to, any training manuals or other training materials.

iv. For each year of the Applicable Time Period, state the number and percentage of clients for which You completed a Compliance Assessment and for which You declined to provide:

    1. a "Compliant" designation on the Attestation of Compliance ("AOC"); or

    2. an "In place" designation on the final Report on Compliance ("ROC").

v. For each year of the Applicable Time Period, state the number and percentage of clients for which You completed a Compliance Assessment and for which You provided:

    1. a "Non-compliant" designation on the AOC; or

    2. a "Not in place" designation on the ROC.

vi. If there is any difference between the answers for questions 3(a)(iv)(1) and 3(a)(v)(1), explain the reason(s) for the difference.

vii. If there is any difference between the answers for questions 3(a)(iv)(2) and 3(a)(v)(2), explain the reason(s) for the difference.

viii. Describe the Compliance Assessment process and provide copies of all policies and procedures related to Compliance Assessment. Your description of the Compliance Assessment process should include, but not be limited to, a discussion of:

1. the bidding process and the process by which you compete for and enter into contracts for Compliance Assessments with clients, including but not limited to how You initiate contact with potential clients and any factors that are negotiated with clients such as price, time for completion, or process for the Compliance Assessment;

2. the staffing of Compliance Assessments, including: (A) the typical number of individuals assigned to a Compliance Assessment, (B) how that number is determined, (C) the professional and training qualifications that each individual assigned to the Compliance Assessment is required to possess, (D) the division of labor between the individuals, and (E) non-Compliance Assessment duties of individuals while they are performing a Compliance Assessment;

3. the typical length of time to complete Compliance Assessments;

4. the Company's pricing structure for Compliance Assessments and typical cost to clients of Compliance Assessments;

5. the method by which the scope of Compliance Assessments is determined, including but not limited to, the extent to which a client or any third party, such as the PCI Security Standards Council ("PCI SSC"), a Payment Card Network, Acquiring Bank, or Issuing Bank, is permitted to provide input into the scoping of Compliance Assessments;

6. the process by which the Company determines whether to use sampling as part of a Compliance Assessment, including, but not limited to, a description of the methodology used to determine that any sample is sufficiently large to assure that controls are implemented as expected. As part of Your response, provide copies of all policies and procedure related to sampling, as well as all documents related to a representative Compliance Assessment that included sampling, including all communications between the Company and the client or any third party, such as PCI SSC, a Payment Card Network, an Acquiring Bank, or an Issuing Bank;

7. the methodology and tools the Company uses to perform Compliance Assessments;

8. the guidelines and policies for interviewing a client's employees as part of a Compliance Assessment. As part of Your response, identify any PCI DSS requirement for which client employee interviews alone could establish whether a client had satisfied the requirement;

9. the policies, procedures, and methodology used by the Company to determine whether a client that has not explicitly met a PCI DSS requirement has implemented an adequate compensating control. As part of Your response, provide copies of all policies and procedures relating to compensating controls, and describe the steps the Company undertakes to determine whether a client has effectively implemented compensating controls;

10. the extent to which the Company communicates with clients in determining the adequacy of any compensating control. As part of Your response, provide all documents related to a representative Compliance Assessment that considered a compensating control, including all communications between the Company and the client or any third party such as PCI SSC, a Payment Card Network, an Issuing Bank or an Acquiring Bank; and

11. the policies and procedures for completing a Report on Compliance ("ROC"), including, but not limited to a discussion of whether a draft report is created, whether that draft is shared with the client or any third party such as PCI SSC, a Payment Card Network, an Issuing Bank or an Acquiring Bank, whether the Company accepts input on the draft from the client or any third party, and whether the Company ever makes changes to the draft report based upon the client or other third parties' input. As part of Your response, provide all documents relating to a representative Compliance Assessment in which You provided a draft of the report to the client and/or any third parties, including a copy of the draft report, any communications with the client or third parties about the draft report, and the final ROC.

ix. Provide: a copy of the Compliance Assessment with the completion date closest to January 31, 2015; and a copy of a Compliance Assessment completed in 2015 that is representative of the Compliance Assessment that the Company performs. For each Compliance Assessment provided in response to this specification, the Company shall also include a copy of any contract with the client for which the Compliance Assessment was performed, all notes, test results, bidding materials, communications with the client and any other third parties, such as the PCI SSC, a Payment

Card Network, an Issuing Bank or an Acquiring Bank, draft reports, the final ROC, and the AOC.

x. State whether the Company ever identifies deficiencies in a client's network during a Compliance Assessment and gives the client the opportunity to remediate the deficiency before the Company completes its final ROC. If so, provide all documents relating to a representative Assessment where the Company gave the client an opportunity to remediate before completing the ROC, including any communications between the Company and the client or any third parties such as PCI SSC, a Payment Card Network, an Issuing Bank or an Acquiring Bank, and the final ROC and AOC.

xi. State whether the Company ever identifies deficiencies in a client's network during a Compliance Assessment and issues a final ROC before the deficiencies are remedied based on assurances that the client will remedy the deficiencies in the future. As part of Your response, provide copies of all policies and procedure related to remedying deficiencies.

xii. State whether the Company has any policies or procedures relating to potential conflicts of interest, including, but not limited to, any policies that prevent the Company from providing Compliance Assessments to clients to which it has also provided another type of service, or that concern the marketing or provision of other services to clients for which You have provided a Compliance Assessment. As part of Your response, provide copies of all relevant policies and procedures.

xiii. State the annual number of the Company's Compliance Assessment clients that have suffered a Breach in the year following the Company's completion of the Assessment for each year of the Applicable Time Period. For each such client, state whether it was subsequently determined not to be PCI compliant and provide the date of the initial Compliance Assessment and any communications between the Company and client or any third parties such as PCI SSC, a Payment Card Network, an Issuing Bank or an Acquiring Bank related to the Breach.

b. **Forensic Audits**

i. State whether the Company provides any Data Security Forensic Audit Services and, if so, describe the services and the length of time that the company has offered these services.

ii. State the Company's annual gross revenue attributable to Data Security Forensic Audit Services for each year of the Applicable Time Period.

iii. State whether the Company has any policies or procedures relating to potential conflicts of interest, including, but not limited to, any policies that prevent the Company from providing Data Security Forensic Audit Services to clients to which it has also provided another type of service or that concern the marketing or provision of other services to clients for which You have provided Data Security Forensic Audit Services. If so, describe these policies and provide copies of all relevant policies and procedures.

4. **Clients**

   a. Provide a copy of a representative client contract for a Compliance Assessment and for Data Security Forensic Audit Services.

5. **Complaints/Inquiries**

   a. State whether the Company has been the subject of any government or regulatory inquiry,private action, arbitration or mediation related to the provision of Data Security Services. Identify each such inquiry or action and describe the nature of the inquiry or action, the practices investigated or at issue, the violations of law investigated or alleged, and the status or outcome of the inquiry or action. For government or regulatory inquiries, identify the agency or entity conducting the inquiry and the name and contact information for the Company's contact person at such agency or entity. For each private action, identify the manner in which the action was resolved and, if applicable, the court in which the action was filed, the date it was filed, and its docket number.

   b. State whether the Company or any individual QSA working for the Company has ever been placed in remediation by the PCI SSC Quality Assurance program. If so provide all documents related to the remediation and steps taken to be returned to good standing, including all communications with PCI SSC.

The Special Report responses called for in this Order are to be filed no later than 45 days from the date of service of this Order.