202-3133

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chairman**
Melissa Holyoak
Mark R. Meador

In the Matter of **GODADDY INC., a corporation, and** **GODADDY.COM, LLC, a limited liability company.**	**DECISION AND ORDER** **DOCKET NO. C-**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents 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 Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit 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 Respondents have violated the Federal Trade Commission Act, 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. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:

    a. Respondent GoDaddy Inc., a Delaware corporation, with its principal office or place of business at 100 South Mill Avenue, Suite 1600, Tempe, Arizona 85281.

    b. Respondent GoDaddy.com, LLC, a Delaware limited liability company with its principal office or place of business at 100 South Mill Avenue, Suite 1600, Tempe, Arizona 85281. GoDaddy.com, LLC is a wholly owned subsidiary of GoDaddy Inc.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Covered Incident" means any incident related to Hosting Services that results in Respondents notifying, pursuant to any Respondent's statutory or regulatory obligation, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

B. "Covered Information" means information collected by any Respondent from or about an individual consumer, including: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other government-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a "cookie," a mobile device ID, or a processor serial number; or (j) login credentials, keys, or certificates used to authenticate to any electronic service.

C. "Hosting Service" means any service that Respondents advertise, promote, offer for sale, sell, or otherwise provide to customers in the United States for the purpose of providing customer access to computer equipment or storage used to host websites, and the computer assets Respondents use in providing or supporting the service.

D. "Managed Hosting Service" means any Hosting Service for which Respondents are responsible for maintaining or updating software, services, or products on behalf of customers.

E. "Respondents" means GoDaddy Inc., a corporation, and its subsidiaries and affiliates incorporated in the United States, and GoDaddy.com, LLC, a limited liability company, and their successors and assigns, individually, collectively, or in any combination.

Provisions

I. Prohibition against Misrepresentations

IT IS ORDERED that Respondents, and Respondents' 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 must not misrepresent in any manner, expressly or by implication:

A. the extent to which they protect the security, confidentiality, integrity, or availability of any Hosting Service;

B. the extent to which they use reasonable or appropriate measures to protect any Managed Hosting Service from unauthorized access;

C. the extent to which they utilize any security technology or technique, including monitoring, to protect any Managed Hosting Service;

D. the extent to which they protect the security, confidentiality, integrity, or availability of any Covered Information; or

E. the extent to which Respondents are members of, adhere to, comply with, are certified by, are endorsed by, or otherwise participate in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including the E.U.-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework.

II. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondents, and any business that Respondents control, directly or indirectly, in connection with the operation of, or provision of access to, any Hosting Service, must, within 90 days after the effective date of this order, establish and implement, and thereafter maintain, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Hosting Service and Covered Information. To satisfy this requirement, Respondents must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Provide the written program and any material evaluations thereof or material updates thereto to Respondents' boards of directors, or a relevant committee thereof, or governing bodies or, if no such board or equivalent governing body exists, to a senior officer of each Respondent responsible for that Respondent's Information Security Program at least once every 12 months and promptly (not to exceed 120 days) following a Covered Incident;

C. Designate a qualified employee to coordinate and be responsible for the Information Security Program;

D. Assess and document, and update at least once every 12 months and promptly (not to exceed 120 days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of any Hosting Service or Covered Information that could result in (1) unauthorized access to any Hosting Service; (2) the unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (3) misuse, loss, theft, alteration, destruction, or other compromise of such information. Respondents must document such an assessment of Managed Hosting Services separately from any other service or environment;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondents identify to the security, confidentiality, or integrity of any Hosting Service or Covered Information identified in response to sub-Provision II.D of this section. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in (1) unauthorized access to any Hosting Service; (2) the unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (3) misuse, loss, theft, alteration, destruction, or other compromise of such information. Respondents must also assume, in designing such safeguards: (1) a high likelihood of unauthorized access to the Hosting Service, due to the number of websites hosted on the Hosting Service; (2) a high risk of harm to customers of the Hosting Service and to users of websites operated by customers of the Hosting Service should unauthorized access to the Hosting Service occur; (3) customers operating websites in the Hosting Service are likely to maintain or collect sensitive information in or through the Hosting Service; and (4) a high risk of unauthorized access to sensitive information maintained on the Hosting Service or collected by customers of the Hosting Service, through websites they operate, should unauthorized access to the Hosting Service occur;

F. Within 90 days of the issuance date of this order, implement, maintain, and document the following security measures:

    1. Implement and maintain centralized system component inventories, including of hardware, software, and firmware elements, that track the out-of-date and vulnerable versions of each Respondent-managed software program, operating system file, and firmware that is installed on any tracked asset, and create an alert for each asset that is using an out-of-date or vulnerable version;

    2. Employ automated tools and mechanisms, such as a security incident and event manager ("SIEM") or equivalent program, to support near real-time analysis of events;

    3. With regard to logging:

        a. Create and retain system audit logs and records collected by Respondents to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity; and

b. Conduct and document, and update at least once every 12 months, an evaluation that considers, at a minimum, (i) industry standards regarding log collection and analysis to support event detections; (ii) event detections available in any SIEM in use by Respondents and the logs necessary to support such detections; and (iii) Covered Incidents from the previous 12 months in order to determine if additional detections are needed and, if so, which logs Respondents should collect and analyze to support such detections;

4. Require that all logins by employees, contractors, and third-party affiliates of Respondents to any Respondent-managed secure shell ("SSH") be authenticated using a method, such as certificates or public/private key pairs, in which at least one component of the credential transmitted to the relying party is not static across multiple authentications, unless such credential is short-lived. In the alternative, Respondents may use widely-adopted industry authentication options that provide at least equivalent security as the authentication method required by the preceding sentence, if the person responsible for the Information Security Program under sub-Provision II.C: (a) approves in writing the use of such equivalent authentication options; and (b) documents a written explanation of how the authentication options are widely adopted and at least equivalent to the security provided by multi-factor authentication;

G. Within 180 days of the issuance date of this order, implement, maintain, and document the following security measures:

1. Disconnect from the Hosting Service environment all hardware assets with Respondent-managed software installed that is no longer supported by a vendor, a Respondent, or other party through the provision of software updates or patches to address vulnerabilities, such as software that is considered end-of-life, or, if disconnection is infeasible, temporarily implement appropriate controls to mitigate threats and document a plan to disconnect the asset or software that includes an appropriate timeline;

2. Use technical measures to detect and prevent anomalous changes to Respondent-managed critical operating system and application files by comparing such files to known baselines, such as file hash values, or, where such baselines are not available, by relying on methods such as non-signature-based technologies, including techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. In the alternative, Respondents may use immutable deployments to prevent unauthorized modifications of any system and application files managed by Respondents that are not monitored using such technical measures;

3. Require at least one multi-factor authentication method for all employees of Respondents and staff of contractors and third-party affiliates in order to access and maintain access (such as through a single sign-on authentication method) to any Hosting Service supporting tool or asset, including connecting to any database. Each

such multi-factor authentication method shall not include telephone call or SMS-based authentication methods and must be resistant to phishing attacks. In the alternative, Respondents may use widely-adopted industry authentication options that provide at least equivalent security as the multi-factor authentication options required by the preceding sentences, if the person responsible for the Information Security Program under sub-Provision II.C: (a) approves in writing the use of such equivalent authentication options; and (b) documents a written explanation of how the authentication options are widely adopted and at least equivalent to the security provided by multi-factor authentication;

4. Require at least one multi-factor authentication method, or widely-adopted industry authentication option that provides at least equivalent security, be provided as an option for customers to authenticate into any Respondent-developed Hosting Service administration tool or database, excluding any SSH or machine-to-machine-only interface, such as an application programming interface ("API"), that does not support multi-factor authentication, including offering customers at least one method that does not require the customer to provide a telephone number, such as by integrating authentication applications or allowing the use of security keys. Any information collected by Respondents from customers for the purpose of enabling multi-factor authentication may only be used for authentication purposes and no other purpose; and

5. Protect any API developed by Respondents that provides access to any Hosting Service configuration or administration or Covered Information by, at a minimum:

    a. Using technical controls to require connections to the API to use HTTPS or an equivalently secure transfer protocol for all requests;

    b. Requiring that all requests to any such API that provides access to Covered Information, including any Hosting Service administration tool that can access Covered Information, be authenticated using a method that protects authenticity at the session level and includes appropriate protections against session hijacking and the insertion of false information into sessions;

    c. Using appropriate rate-limiting for connections to the API; and

    d. Monitoring inbound and outbound API communications traffic, to detect attacks and indicators of potential attacks;

H. Assess, at least once every 12 months and promptly (not to exceed 120 days) following a Covered Incident, the sufficiency of any safeguards and security measures in place to address the internal and external risks to the security, confidentiality, or integrity of Hosting Services and Covered Information, and modify the Information Security Program as needed based on the results;

I. Test and monitor the effectiveness of the safeguards and security measures at least once every 12 months and promptly (not to exceed 120 days) following a Covered Incident,

and modify the Information Security Program as needed based on the results. Such testing and monitoring must include vulnerability scanning of Respondents' network(s) at least once daily, penetration testing of Respondents' network(s) at least once every 12 months, and, in the event of a Covered Incident, a security assessment or penetration testing of affected systems promptly (not to exceed 120 days) following the Covered Incident;

J. Select and retain service providers capable of safeguarding Hosting Services and Covered Information they access through or receive from Respondents, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Hosting Services and such Covered Information;

K. Evaluate and adjust the Information Security Program as needed in light of any changes to Respondents' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision II.D of this Order, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards or security measures. At a minimum, Respondents must evaluate the Information Security Program at least once every 12 months and modify the Information Security Program as needed based on the results; and

L. Either during the due diligence process of the acquisition of any entity ("Acquired Entity") that would become part of any Hosting Service or following such acquisition, Respondents must assess the Acquired Entity's safeguards and independently test the effectiveness of the safeguards to protect from unauthorized access any Hosting Service of which the Acquired Entity would become a part. Respondents shall not integrate any of the Acquired Entity's application or information systems into any Respondent's network until (1) all material risks to the security, confidentiality, and integrity of any Hosting Service identified in such a test are remediated; and (2) such application or information system meets the requirements of this Provision. *Provided, however,* that Respondents shall have 90 days after integrating any application or information system of an Acquired Entity into its networks to implement the requirements of sub-Provision II.G.4 with respect to such application or system.

III. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Information Security Program, Respondents must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; (3) designates all documents relevant to each Assessment for retention for 5 years after completion of such Assessment, and (4) provides any such documents to the Commission within 10 days of receipt of a written request from a representative of the

Commission. If the Assessor had access to a document by an electronic means controlled by Respondents, such as a fileshare or repository, to which the Assessor no longer has access, the Assessor must identify the document for production by Respondents as it existed at the time the Assessor had access to it. No document may be withheld from the Commission by the Assessor, or by any Respondent if previously provided to the Assessor, on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory protection, or any similar claim.

B. For each Assessment, Respondents must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 12 months after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for 20 years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondents have implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of Respondents' implementation and maintenance of sub-Provisions II.A-L; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and (5) identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondents' management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondents' management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Respondents revise, update, or add one or more safeguards required under Provision II of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within 90 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed via email to DEbrief@ftc.gov or 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, Washington, DC 20580. The subject line must begin, "In re GoDaddy Inc., C-####." All subsequent biennial Assessments must be retained by Respondents until the order is terminated and provided to the Associate Director for Enforcement within 10 days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

IV. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondents, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondents' network(s) and all of Respondents' IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondents have implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-L; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

V. Annual Certification

IT IS FURTHER ORDERED that Respondents must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior executive officer of each Respondent with responsibility over information security that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior executive officer or any senior corporate manager, senior officer, or subject matter experts upon whom the senior executive officer relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or 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, Washington, DC 20580. The subject line must begin, "In re GoDaddy Inc., C-####."

VI. Covered Incident Reports

IT IS FURTHER ORDERED that, within 10 days of any notification to a United States federal, state, or local entity of a Covered Incident, the Respondent that experienced such Covered Incident must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of consumers or businesses whose information, account, or website was affected by the Covered Incident;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Hosting Services and Covered Information from further exposure or access, and protect affected individuals and businesses from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Respondent to consumers or businesses or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports 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, Washington, DC 20580. The subject line must begin, "In re GoDaddy Inc., C-####."

VII. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

A. Each 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 the issuance date of this Order, each Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in

structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur within 10 days of when they assume their responsibilities.

C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order, which may be obtained through a Digital Signature. Digital Signature means the result of a cryptographic transformation of data that is properly implemented to provide the services of origin authentication, data integrity, and signer non-repudiation.

VIII. Compliance Report and Notices

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

A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which each 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 that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent; (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any 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. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such 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, Washington, DC 20580. The subject line must begin: In re GoDaddy Inc., C-####.

IX. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondents, in connection with the provision of Hosting Services, must create and retain the following records:

A. accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

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 written or electronic consumer complaints stored in any Respondent's applicable system of record, in connection with Hosting Services, concerning information security, data privacy, or any privacy or security program sponsored by a government or self-regulatory or standard-setting organization of which any Respondent is a member, whether received directly or indirectly, such as through a third party, and any written or electronic response;

D. a copy of each materially different advertisement or other marketing material making a representation subject to this Order;

E. a copy of each widely disseminated, materially different representation by Respondents that describes the extent to which Respondents maintain or protect the privacy, security and confidentiality of any Hosting Services and Covered Information, including any representation concerning a change in any service controlled by Respondents that relates to the privacy, security, and confidentiality of any Hosting Service or Covered Information;

F. for 5 years after the date of preparation of each Assessment required by this Order, all relevant documents, including each document designated by the Assessor, as each existed at the time the Assessor had access to it; all documents relied upon to prepare the Assessment, even if prepared by a third party on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments; and any other documents concerning Respondents' compliance with related Provisions of this Order; and

G. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

X. Compliance Monitoring

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

A. Within 10 days of receipt of a written request from a representative of the Commission, each 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 each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any 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 Respondents or any individual or entity affiliated with Respondents, without the necessity of 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.

XI. 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 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an 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 any 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.

April J. Tabor
Secretary

SEAL:
ISSUED: