202-3133

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Lina M. Khan, Chair
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

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

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

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,

[illegible] 008 T4c 0 Tw143.22 -F2.3 Td(E.)TjEMC /Spanite/MCID 10 >

E.

such multi-factor authentication method shall not include telephone call or SMS-based authentication methods and must be resistant to phishing attacks. In the

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

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

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

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 Respos sto25 -1.1e reaso a mervice; s 2w 8.

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 terminat

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: