**Analysis of Proposed Consent Order to Aid Public Comment**
***In the Matter of GoDaddy Inc.* File No. 2023133**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from GoDaddy Inc. and GoDaddy.com, LLC ("Respondents").

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

Respondent GoDaddy Inc. is a Delaware corporation with its headquarters in Arizona. Respondent GoDaddy.com, LLC is a Delaware limited liability company with its headquarters in Arizona and is a wholly owned subsidiary of GoDaddy Inc. Respondents provide website hosting services to individuals and businesses of all sizes, including small businesses.

Since at least 2015, the Commission alleges, Respondents have marketed their services as a secure choice for customers to host their websites, touting their commitment to data security. Respondents have also stated that they comply with the Privacy Shield Framework principles, which include a promise to take reasonable and appropriate measures to protect the security of personal information.

As alleged in the complaint, in fact, Respondents' data security practices were not reasonable for their size and complexity. GoDaddy did not have reasonable visibility into vulnerabilities and threats affecting its hosting services. Since 2018, GoDaddy has failed to implement standard security tools and practices to protect its hosting services and to monitor them for security threats. In particular, GoDaddy allegedly failed to: (a) inventory and manage assets; (b) manage software updates; (c) assess risks to its website hosting services; (d) use multi-factor authentication; (e) log security-related events; (f) monitor for security threats, including by failing to use software that could actively detect threats from its many logs, and failing to use file integrity monitoring; (g) segment its network; and (h) secure connections to services that provide access to consumer data. In light of these failures, the Commission challenged GoDaddy's representations about security and adhering to the Privacy Shield Framework principles as false or misleading.

As a result of Respondents' data security failures, as alleged in the complaint, they experienced several incidents of unauthorized access to their hosting service between 2019 and December 2022, in which threat actors repeatedly gained access to customers' websites and data, causing harm to Respondents' customers and putting them and visitors to the customers' websites at risk of further harm.

The Commission's proposed three-count complaint alleges that Respondents engaged in unfair and deceptive practices in violation of Section 5(a) of the FTC Act by (1) unfairly failing to employ reasonable and appropriate data security measures, (2) deceptively representing that

they used reasonable and appropriate data security measures, and (3) deceptively representing that they adhere to the EU-U.S. and/or Swiss-U.S. Privacy Shield Principles.

With respect to the first count, the proposed complaint alleges that Respondents failed to employ reasonable and appropriate measures to protect their hosting environment from unauthorized access. Respondents' failure to employ such reasonable and appropriate measures has caused or is likely to cause substantial injury to consumers in the form of several data breaches between 2019 and 2022, theft of Respondents' customers' confidential information stored in Respondents' hosting services, and alteration of Respondents' customers' websites. These injuries are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers themselves.

**Summary of Proposed Order with Respondents**

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

**Provision I** prohibits Respondents from misrepresenting, expressly or by implication: (1) the extent to which they protect the security, confidentiality, integrity, or availability of their hosting services; (2) the extent to which they use reasonable or appropriate measures to protect certain hosting services from unauthorized access; (3) the extent to which they utilize any security technology or technique, including monitoring, to protect certain hosting services; (4) the extent to which they protect the security, confidentiality, integrity, or availability of consumers' personal information; and (5) the extent to which Respondents are a member 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.

**Provision II** requires that Respondents establish, implement, and document a comprehensive information security program. The program must include specific security measures tailored to Respondents' previous data security shortcomings alleged in the complaint.

**Provisions III-VI** require that Respondents obtain initial and biennial information security assessments by an independent, third-party professional for 20 years (Provision III), cooperate with the independent assessor (Provision IV), provide the Commission with annual certifications of compliance with the Order from a senior executive officer from each Respondent (Provision V), and submit reports to the Commission if they suffer additional data incidents (Provision VI).

**Provisions VII-X** are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance.

**Provision XI** states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.