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.**	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission, having reason to believe that GoDaddy Inc., a corporation, and GoDaddy.com, LLC, a limited liability company (collectively, "GoDaddy" or "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

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

2. Respondent GoDaddy.com, LLC ("GoDaddy.com") is 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 is a wholly-owned subsidiary of GoDaddy Inc.

3. Respondents have advertised, offered for sale, sold, and distributed products to consumers, including domain name and website hosting services.

4. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Summary of the Case

5. GoDaddy is one of the largest website hosting companies in the world, with approximately five million customers. Since at least 2015, GoDaddy has marketed itself as a secure choice for customers to host their websites, touting its commitment to data security and

careful threat monitoring practices in multiple locations, including its main website for hosting services, its "Trust Center," and in email and online marketing.

6. In fact, GoDaddy's data security program was unreasonable for a company of its size and complexity. Despite its representations, GoDaddy was blind to vulnerabilities and threats in its hosting environment. Since 2018, GoDaddy has violated Section 5 of the FTC Act by failing to implement standard security tools and practices to protect the environment where it hosts customers' websites and data, and to monitor it for security threats. In particular, GoDaddy 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. These failures made GoDaddy's representations about security false or misleading.

7. As a result of GoDaddy's data security failures, it experienced several major compromises of its hosting service between 2019 and December 2022, in which threat actors repeatedly gained access to its customers' websites and data, causing harm to its customers and putting them and visitors to their websites at risk of further harm. GoDaddy's customers and other consumers could not avoid this harm, and it is not outweighed by benefits to consumers or competition. Even after these compromises of its environment, GoDaddy continues to struggle to gain visibility into its hosting environment and adequately monitor it for threats.

GoDaddy's Website Hosting Services

8. To provide its website hosting services, GoDaddy provides services and computer storage to customers to enable them to run their own websites. GoDaddy owns and operates hundreds of thousands of computer servers. GoDaddy also contracts for server space from Amazon Web Services for certain services it offers.

9. GoDaddy provides website hosting to individuals and businesses of all sizes. For some services, GoDaddy provides customers dedicated portions of GoDaddy's computer environment—either physical or virtual servers—which customers manage themselves and for which the customers have administrative privileges and responsibility ("Customer-Managed Hosting"). These customers are responsible for updating the software running in their virtual servers, and in most cases GoDaddy does not have administrative privileges to the servers. But many other GoDaddy customers run their websites in portions of GoDaddy's environment that are shared with other customer sites ("Shared Hosting"), for which GoDaddy maintains administrative privileges and responsibility for updating the software it provides, including the operating system and website management software. The typical customers of GoDaddy's Shared Hosting services are small businesses.

10. GoDaddy offers its Shared Hosting customers common website management software produced by third parties to run their websites, including cPanel, WordPress, and Plesk. GoDaddy divides its Shared Hosting environment into discrete portions for each website management software (i.e., GoDaddy's "cPanel service" and "WordPress service"). GoDaddy also offers accompanying services, such as payment processing, add-on features, backup

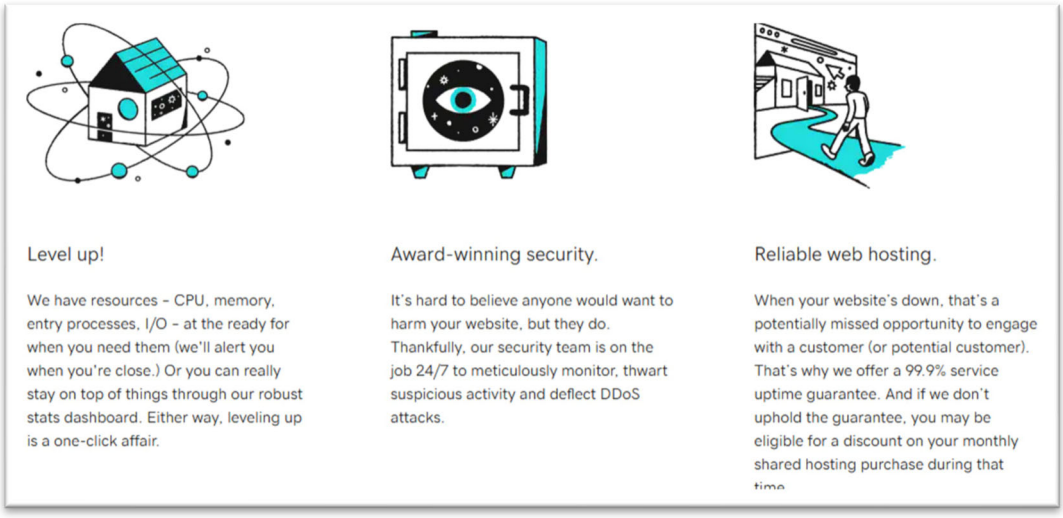
services, and assistance in managing customers' websites. GoDaddy's customers store data necessary to run their websites on GoDaddy's servers.

11. GoDaddy Inc. has directly participated in the security practice failures at issue. For example, when GoDaddy Inc. acquired a European hosting company, Host Europe Group ("HEG"), it made GoDaddy.com responsible for HEG's security. Many of HEG's servers were no longer receiving security patches for their software, introducing security risks into GoDaddy.com's Shared Hosting environment. By directing GoDaddy.com to take responsibility for these servers, GoDaddy Inc. added security obligations to GoDaddy.com's security team, and introduced a risk of vulnerabilities that could be exploited by threat actors.

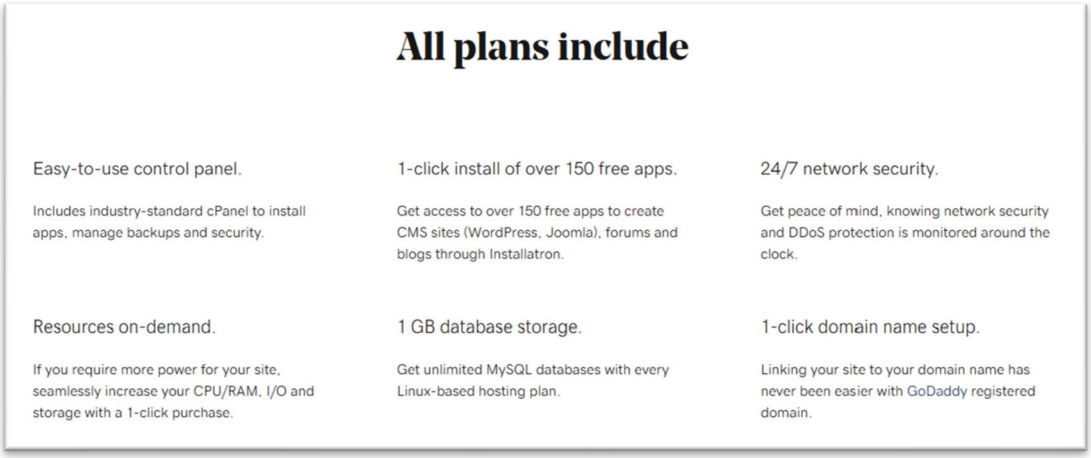
Data Security Representations

12. GoDaddy has disseminated or has caused to be disseminated advertisements, promotional materials, and other representations regarding data security for its Shared Hosting services, including but not necessarily limited to the attached Exhibits A through E. These materials contain the following statements and depictions:

a.

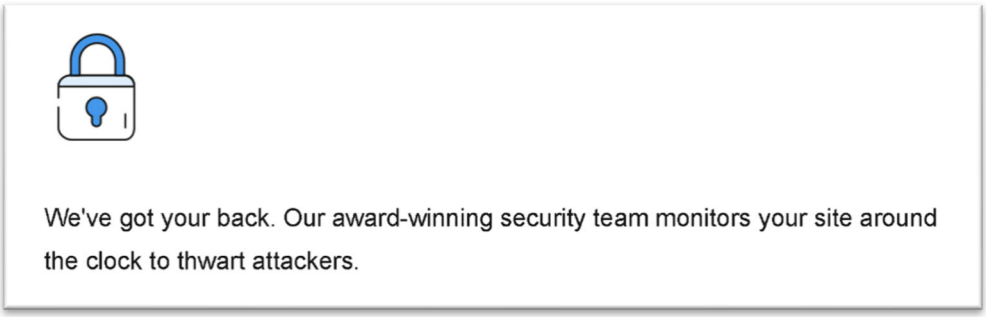


and



(Exhibit A, GoDaddy.com Hosting Landing Page (Sept. 2020)).

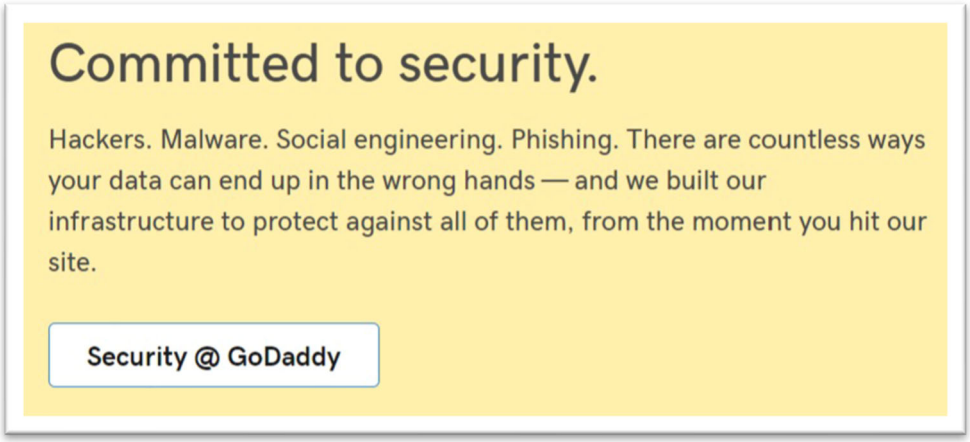
b.



(Exhibit B, GoDaddy Marketing Email Template (2017, 2018, 2021)).

c.

and



(Exhibit C, GoDaddy Trust Center Landing Page (Mar. 2019)).

d.

(Exhibit D, Trust Center Security Landing Page (Mar. 2019)).

e.

(Exhibit E, Facebook advertisement (May-Aug. 2020)).

Privacy Shield Representations

13. The Department of Commerce ("Commerce") and the European Commission negotiated the EU-U.S. Privacy Shield framework to provide a mechanism for companies to transfer personal data from the European Union to the United States in a manner consistent with the requirements of European Union law on data protection. The Swiss-U.S. Privacy Shield framework is identical to the EU-U.S. Privacy Shield framework.

14. To join the EU-U.S. and/or Swiss-U.S. Privacy Shield framework, a company must certify to the United States Department of Commerce that it complies with the Privacy Shield Principles. Participating companies must annually re-certify their compliance. The Privacy Shield frameworks expressly provide that, while decisions by organizations to "enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles."

15. Companies under the jurisdiction of the FTC are eligible to join the EU-U.S. and/or Swiss-U.S. Privacy Shield framework. Both frameworks warn companies that claim to have self-certified to the Privacy Shield Principles that failure to comply or otherwise to "fully implement" the Privacy Shield Principles "is enforceable under Section 5 of the Federal Trade Commission Act."

16. The Privacy Shield Principles include the following:

> SECURITY [Principle 4]: (a) Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

17. GoDaddy provided an EU-U.S. Privacy Shield certification to the United States Department of Commerce in January 2017, a Swiss-U.S. Privacy Shield certification in August 2018, and it has annually recertified since that time.

18. Since no later than March 2018, GoDaddy has represented to consumers that it complies with the Privacy Shield Principles. For example, a former GoDaddy privacy policy stated that it "participates in and has certified its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Framework." (Exhibit F, Excerpt of GoDaddy Privacy Policy (Mar. 26, 2018)). And, since February 2021, GoDaddy has stated publicly that it "has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles." (Exhibit G, Excerpt of GoDaddy Privacy Policy (May 3, 2023)).

19. Although the European Court of Justice determined on July 16, 2020 that the EU-U.S. Privacy Shield framework was not adequate for allowing the lawful transfer of personal data from the European Union, and the Swiss Data Protection and Information Commissioner determined on September 8, 2020 that the Swiss-U.S. Privacy Shield framework was similarly inadequate, those decisions do not change the fact that GoDaddy has represented to consumers

that it has certified its compliance with both Privacy Shield frameworks, and as such, would fully comply with the Principles, including the Security Principle (Principle 4).

Data Security Failures

20. Server environments such as GoDaddy's Shared Hosting environment are subject to several forms of well-known threats. In a 2018 blog post, GoDaddy noted several of these threats:

> Some of the most common threats website owners face today are:
>
> - **Your website redirects to a malicious website.** This often occurs when malware finds a "backdoor" into a website's code and then redirects the website elsewhere. Often, these backdoors allow attackers to retain and regain access to a website to continue their nefarious acts.
>
> - **Data collection.** Any place data is transmitted over your website, hackers want to gain access and collect that information.
>
> - **Mailer script infections.** If there is a contact form on your website, your information and the contact information of your patrons could be vulnerable without the right precautions.
>
> - **Database attacks.** Many websites utilize a database, which may be prone to attacks without the proper protection.
>
> - **User authentication.** Without the right configuration, your user's authenticated sessions could be vulnerable.
>
> - **Outdated plugins and code.** These allow hackers to modify and manipulate your website files.
>
> - **DDoS attacks.** Distributed Denial of Service attacks are used to cripple a website by overwhelming it with "fake traffic," preventing true visitors from accessing your website.

21. Since at least January 2018, GoDaddy has engaged in numerous practices that, taken individually or together, failed to provide reasonable security in its Shared Hosting environment to prevent unauthorized access and to protect it from such threats, as follows:

a. GoDaddy has failed to adequately inventory and manage computer assets. GoDaddy has not formally defined or documented its asset management processes, and its tracking of assets has been spread across multiple tools. GoDaddy's main tool was a configuration management database ("CMDB"). But as of September 2020, GoDaddy only had visibility into approximately 15,000 devices, out of approximately 450,000 it ultimately identified when it fully populated its CMDB over 2020 and 2021. In addition, GoDaddy has failed to centrally track and inventory software.

b. GoDaddy has failed to adequately manage security-related software updates (also called patches):

    i. GoDaddy has failed to centrally track whether operating systems and other software are current with necessary security patches. Prior to 2020, GoDaddy's security policy required critical security patches to be installed within 30 days. But, up until 2022, it relied on various product teams to install patches with no means to centrally track whether they had done so. As a result, GoDaddy's installation of patches has been inconsistent, and on numerous occasions available patches have not been installed, subjecting the devices to known critical vulnerabilities. Only after GoDaddy discovered a major security compromise of the Shared Hosting environment in 2020 did it begin to install software that would enable it to centrally view and manage patch status. Installation of this software across the majority of the environment was not complete until December 2021.

    ii. Also, prior to 2020, GoDaddy did not have adequate procedures for retiring operating systems prior to their end-of-life date, the date after which software providers stop providing security patches. Despite maintaining patching standards that specified the minimum acceptable version of operating systems (i.e., not end-of-life), GoDaddy did not enforce those standards sufficiently. GoDaddy delegated the responsibility for patching to business unit staff without means of ensuring compliance, allowed for alternatives to retiring end-of-life servers, and integrated servers into its environment that violated its patch standard. As a result, as of the fall of 2019, GoDaddy had 30,000 end-of-life servers in the Shared Hosting environment, with no plan to address them, and no central way to track where they were. From 2020 to the present, GoDaddy reduced its number of end-of-life systems and acquired extended patch support for a third of those, but it has not entirely resolved the issue.

c. GoDaddy has failed to adequately assess risks to its Shared Hosting environment. For example:

    i. GoDaddy has failed to conduct regular penetration testing for the Shared Hosting environment. Penetration testing evaluates how secure an environment is against unauthorized access or exploitation by attempting to compromise it. Since 2015, GoDaddy conducted a single penetration test for each segment of the Shared Hosting environment, which failed to identify the vulnerabilities described in (h) and (i) below. More frequent testing improves the likelihood that testing finds such issues, because environments change, and testers can catch additional issues with further testing.

    ii. When assessing risks, GoDaddy has failed to adequately consider the type and sensitivity of information in its Shared Hosting environment. For example, the risk assessments GoDaddy conducted for its cPanel service excluded any consideration of the types of information that GoDaddy's customers did or might store or process through their websites.

d. GoDaddy has failed to adequately log security-related events and information. Until at least 2020, GoDaddy's logging of events was ad hoc and inconsistent, and its logging practices did not follow its written policies. Even where logging did occur, GoDaddy failed to consistently store logging data in its central log repository (the archive for historic log data). As a result, GoDaddy security staff could not readily access logged information to analyze or investigate suspicious activity. And GoDaddy failed to consistently retain logs for enough time to enable investigation, in some cases for only seven days or not at all, in contravention of its own policies that required logs to be retained for at least a year.

e. GoDaddy has failed to adequately monitor for suspicious activity and security threats:

    i. GoDaddy has failed to utilize a security incident and event manager ("SIEM") with the capability to detect and alert GoDaddy to suspicious activity:

        1. Prior to 2020, GoDaddy would only perform manual, ad hoc reviews of cPanel logs. Due to the scope and volume of GoDaddy's operations, this type of review was insufficient for any type of proactive monitoring.

        2. Although GoDaddy utilized various SIEM or SIEM-like programs to aggregate some logged information, its SIEM was not set up to detect and alert on potential security events until the Spring of 2020, when GoDaddy first created alerts to detect the activities of a threat actor that had compromised the Shared Hosting environment. As of Spring 2022, GoDaddy still had not fully integrated the SIEM's detection and alerting capabilities across the Shared Hosting environment.

    ii. GoDaddy does not use file integrity monitoring in the Shared Hosting environment. File integrity monitoring compares operating system and application software files against known benchmark files to ensure that they have not been corrupted, altered, or replaced without the organization's approval.

    iii. GoDaddy has also failed to implement alternative security controls or monitoring tools to compensate for the absence of a SIEM with detection capability or file integrity monitoring. For example, GoDaddy has not made it a regular practice to conduct threat hunting—proactively searching for threats that may be undetected in a network—as part of its ongoing security program. GoDaddy also did not begin to install endpoint detection and response tools in the Shared Hosting environment until October 2022, and it still has not fully implemented this solution. And GoDaddy has not implemented alternatives to real-time file integrity monitoring, such as creating and monitoring honeypots (decoy servers that are set up to attract threat actors), to which it could deploy a file integrity monitoring solution to detect widespread compromises.

f. GoDaddy has relied on username/password authentication for employee SSH access to customer environments, such as its cPanel service, instead of a more secure alternative such as SSH certificates or public/private key pairs.

g. GoDaddy has failed to implement multi-factor authentication ("MFA"). Until after it discovered a breach of its cPanel service in March 2020, GoDaddy did not require MFA for privileged, employee administrative logins to the environment. GoDaddy has also not offered MFA as an option to customers for their cPanel administration logins.

h. GoDaddy has failed to adequately segment its Shared Hosting environment from less-secure portions of its network such as its Customer-Managed Hosting service. GoDaddy cannot ensure that its Customer-Managed Hosting customers apply security patches in a timely fashion, and thus cannot ensure that customers' virtual servers do not suffer from known security vulnerabilities. Yet, until at least April 2020, GoDaddy connected its Shared Hosting and Customer-Managed Hosting environments with a third product environment via a specialized type of server that GoDaddy had configured to allow communication in both directions. GoDaddy thus exposed its Shared Hosting customers to the security weaknesses of its most careless Customer-Managed Hosting customers, and a threat actor in fact exploited this weakness to move between environments, as noted below. GoDaddy did not maintain any policy prohibiting this configuration, document its risks, or implement additional security controls to mitigate the risk.

i. GoDaddy has failed to secure connections to services, such as application programming interfaces ("APIs"), that provide access to consumer data:

    i. For its Managed WordPress service, another portion of the Shared Hosting environment, GoDaddy created an internet-facing API. The internally developed API enables customer service staff to retrieve sensitive information pertaining to customers of GoDaddy's Managed WordPress service, part of the Shared Hosting environment, including several kinds of login credentials and private encryption keys. The API does not require MFA, and GoDaddy has not secured connections to the API with certificates, which is a standard practice to ensure that only authorized users or services connect to it.

    ii. The API used an authentication method called basic authentication, which sends unobscured, plaintext login credentials during the authentication process. Additionally, prior to February 2022, the API failed to force connections to encrypt web traffic, which means that if any application connecting to the API did not use HTTPS—the standard encryption for web traffic—the traffic to and from the API, including login credentials, was also not encrypted. Unencrypted login credentials are susceptible to machine-in-the-middle attacks, in which a threat actor inserts themselves into communication between two parties, intercepting the targets communications and potentially altering them. In such an attack, a threat actor could intercept the unencrypted credentials and use them to further compromise the environment.

    iii. In addition, GoDaddy has failed to implement supplemental security controls for the API, such as restricting access to trusted connections using an application firewall, rate-limiting connections to the API, or otherwise alerting on anomalies.

Compromises of GoDaddy's Shared Hosting Environment

22. In October 2019, a threat actor gained access to the Shared Hosting environment. The threat actor likely took advantage of an unpatched vulnerability in the Customer-Managed Hosting environment, where customers were responsible for patching. The threat actor then moved laterally into the Shared Hosting environment through a specialized type of server that connected these two environments with a third product environment. During later investigation, GoDaddy's security team discovered that over a third of the 254 such specialized servers it operated were running software with known vulnerabilities, and the threat actor had exploited these vulnerabilities to replace server files with malicious versions on seventeen of them, exactly the type of activity that file integrity monitoring is designed to detect. The threat actor was likely able to use this access to move into the Shared Hosting environment.

23. In late March 2020, a threat actor's actions inside GoDaddy's network caused GoDaddy's front page website to go down. Although this threat actor was not definitively linked to the first threat actor, the website interruption prompted GoDaddy to hire an outside security firm to search its networks for possible compromise, including the Shared Hosting environment. At this point, the initial threat actor had been in the Shared Hosting environment for six months, yet GoDaddy had not been alerted by any of its security tools or monitoring systems. In addition, due to its insufficient logging and monitoring, GoDaddy was unable to determine how the threat actor initially gained entry to the environment.

24. In April 2020, the security firm discovered that several types of application files in servers belonging to GoDaddy's cPanel service, part of the Shared Hosting environment, had been replaced with malicious versions. These malicious application files recorded the login information cPanel customers used to administer their websites, called Secure Shell or SSH credentials. The threat actor was able to replace one type of file with a malicious version on approximately 45,000 cPanel servers. The threat actor compromised approximately 28,000 customer SSH credentials and 199 employee SSH credentials, which GoDaddy staff use to manage the Shared Hosting environment. The employee SSH credentials did not require MFA, so the threat actor was able to make administrative changes to the environment using the compromised SSH credentials.

25. As GoDaddy attempted to remove the threat actor's access, the threat actor pivoted techniques and began to replace a different type of server application file. The malicious version of the new file type scanned traffic to the server for credit or debit card information, ultimately capturing approximately 1,000 card numbers that customers were processing in the Shared Hosting environment, contrary to GoDaddy's terms of use.

26. In response to the incident, GoDaddy reset the 28,000 affected customers' SSH credentials, requiring the customers to change their credentials to new ones, and notified them of the incident. GoDaddy also worked to notify consumers who had their card data compromised and offered them credit monitoring.

27. In November 2021, a spike in customer inquiries alerted GoDaddy to a compromise of its WordPress Managed Hosting service in the Shared Hosting environment. A threat actor used previously compromised credentials to access an internet-facing API that enabled customer

service staff to retrieve information on GoDaddy's customers. The API could be queried for several types of data: (1) customers' email addresses; (2) private encryption keys; and (3) three types of credentials—their WordPress administration credentials; credentials to a database where the customer could store data associated with their site; and their secure File Transfer Protocol credentials, which customers use to upload files to their sites. GoDaddy used sequential customer IDs for each customer account, enabling the threat actor to easily query for additional customers' data. The threat actor queried the API for 1.2 million customers' data, including data of nearly 700,000 customers in the United States. Because of its limited logging practices, GoDaddy was unable to determine which data elements the threat actor accessed for each customer.

28. The threat actor used the stolen credentials to commit search engine optimization fraud by installing a webshell to some customers' WordPress websites. The webshell allowed the threat actor to implant code that would falsely tell a search engine that, when someone clicked on a link for the compromised site, it was a different website that had been selected, boosting the other site's ranking.

29. In remediating the Managed WordPress incident, GoDaddy placed the API behind an application firewall so it could not be accessed from the internet, but it has since removed that protection. GoDaddy notified the affected customers, reset their credentials, and revoked the certificates associated with potentially compromised private keys. GoDaddy attempted to rekey the certificates on its customers' behalf, and, where it could not, provided instructions on how to do so.

30. In December 2022, GoDaddy discovered that a threat actor—who GoDaddy believes to be the same threat actor from the 2019-2020 compromise of its cPanel service—had again compromised parts of its cPanel service. The threat actor used a compromised file that GoDaddy had not removed in remediating the previous compromise. Using this file, the threat actor regained access to the Shared Hosting environment and used that access to steal customer SSH credentials *again*. This time, the threat actor used its access to redirect some visitors to customers' websites to sites of the threat actor's choosing, such as websites claiming the customer had committed copyright infringement or websites featuring pornography. Due to its insufficient security monitoring, GoDaddy again failed to proactively detect this compromise, and was instead alerted by customer inquiries.

31. In addition to the harm perpetrated in the compromises described above, GoDaddy's security failures are likely to cause harm to consumers, including GoDaddy's customers and visitors to the customers' websites. GoDaddy's failures enabled threat actors to gain a level of access to the Shared Hosting environment that they are likely to use to harm consumers, regardless of the mode they choose:

a. For example, the threat actors who compromised the Shared Hosting environment had access to any confidential information that GoDaddy's affected customers maintained in the Shared Hosting environment, including any personally identifiable information they maintained on or on behalf of their own customers.

b. The compromises described above left consumers vulnerable to numerous harms, such as threat actors altering GoDaddy's customers' websites in ways that harm their businesses, installing malware to steal sensitive information related to the site owners' customers, and implanting malicious code on the websites that harms consumers visiting those websites. Malicious code on these websites is likely to subject visitors to viruses or other compromises of their personal computers, which in turn is likely to lead to theft of consumers' personal or financial information and other harm, such as ransomware attacks, identity theft, and, at a minimum, significant time spent remediating computer viruses.

c. Furthermore, threat actors in any of the compromises described above would have been able to redirect unsuspecting website visitors to malicious websites, as they did in the December 2022 compromise. Threat actors can send consumers to sites set up to steal their personal or financial information, leading to identify theft or financial fraud.

32. GoDaddy's Shared Hosting customers have also spent time and effort protecting themselves from the consequences of GoDaddy's practices, including time spent resetting account credentials, restoring compromised websites and certificates, addressing their own customers' concerns, and other remediation in light of the security incidents described above.

33. GoDaddy's Shared Hosting customers are not able to avoid the consequences of GoDaddy's security failures. Shared Hosting customers do not know detailed information about GoDaddy's security controls, including which security controls or tools GoDaddy does not use in its Shared Hosting environment. In addition, as described in Paragraphs 12-19, GoDaddy has represented that it provided reasonable security for the Shared Hosting environment, and that it meticulously monitored the environment for security threats.

34. Consumers who have interacted with GoDaddy's customers' websites have also not been able to avoid the consequences of GoDaddy's security failures. In most cases, consumers who visit GoDaddy's customers' sites are unaware that they are interacting with a site or service hosted by GoDaddy.

35. The harm that GoDaddy's security failures have caused or are likely to cause is not offset by countervailing benefits to consumers or competition. GoDaddy could have remediated its failures using well-known and low-cost technologies and techniques.

Count I
Unfair Data Security Practices

36. As described in Paragraphs 20-35, GoDaddy's failure to employ reasonable and appropriate measures to protect the Shared Hosting environment from unauthorized access has caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count II
Data Security Misrepresentations

37. As described in Paragraph 12, GoDaddy has represented, directly or indirectly, expressly or by implication, that it has used reasonable and appropriate measures to protect the Shared Hosting environment against unauthorized access.

38. In fact, as set forth in Paragraphs 20-30, GoDaddy has not used reasonable and appropriate measures to protect the Shared Hosting environment against unauthorized access. Therefore, the representation set forth in Paragraph 37 is false or misleading.

Count III
EU-U.S. & Swiss-U.S. Privacy Shield Frameworks

39. As described in Paragraphs 13-19, GoDaddy has represented, directly or indirectly, expressly or by implication, that it adheres to the EU-U.S. and/or Swiss-U.S. Privacy Shield Principles, including the Security Principle (Principle 4).

40. In fact, as described in Paragraphs 20-30, GoDaddy has not adhered to the Security Principle (Principle 4). Therefore, the representation set forth in Paragraph 39 is false or misleading.

Violations of Section 5

41. The acts and practices of GoDaddy as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 2025, has issued this Complaint against GoDaddy.

By the Commission.

April J. Tabor
Secretary

SEAL: