202-3133

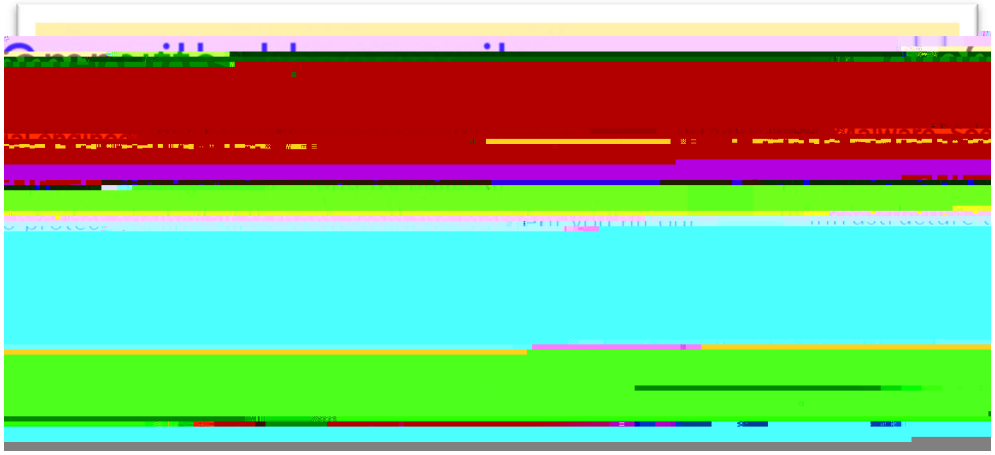
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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.**

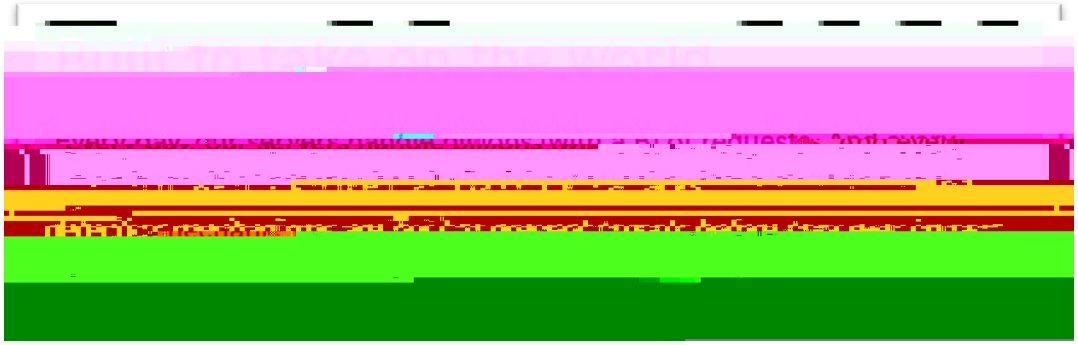
COMPLAINT

Summary of the Case



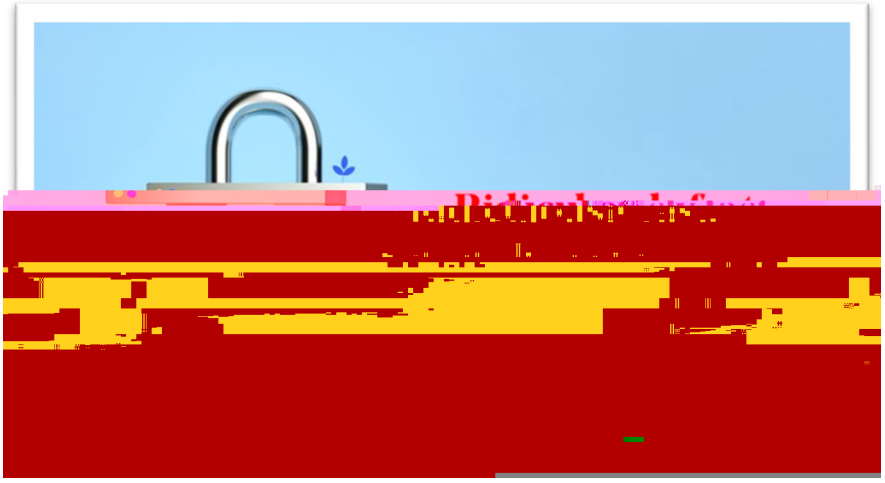
(Exhibit C, GoDaddy Trust Center Landing Page (Mar. 2019)).

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")

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 and SH 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

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 SIM 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 servers, instead of a more secure alternative such as SSH certificates or public/private key pairs.

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 _____, 202 , has issued this Complaint against GoDaddy.

By the Commission.

April J. Tabor
Secretary

SEAL: