172 3003

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of	)	
	)	**DOCKET NO. C-4678**
James V. Grago, Jr., individually and d/b/a ClixSense.com	)	

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that James V. Grago, Jr., individually and doing business as ClixSense.com, a sole proprietorship ("Respondent"), has violated the provisions of the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent is James V. Grago, Jr. ("Grago"), individually and doing business as ClixSense.com ("ClixSense"), which operates as a sole proprietorship with its principal office or place of business in Hampstead, North Carolina. Respondent Grago is the sole owner of ClixSense. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices alleged in this complaint.

2. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

RESPONDENT'S BUSINESS ACTIVITIES

3. Since 2010, Respondent Grago has owned and operated ClixSense. ClixSense generated revenues of $6.7 million in 2015 and $9.1 million in 2016. ClixSense's users are individual consumers who earn money from ClixSense by viewing advertisements, performing online tasks, or completing online surveys.

4. As part of the enrollment process, Respondent collects and stores personal information on ClixSense's computer network about its users, including full names, physical addresses,

dates of birth, gender, and email addresses. Respondent also requires users to create a username, a password, and an answer to a security question that it stores in its database.

5. Respondent requires that users who earn more than $600 annually from ClixSense provide Respondent with their Social Security numbers.

6. In total, Respondent stores or has stored personal information, including Social Security numbers, for approximately 6.6 million consumers.

RESPONDENT'S DECEPTIVE PRACTICES

7. Since at least 2011, Respondent has disseminated or caused to be disseminated the following statement, among others, regarding the security measures ClixSense takes to protect personal information. (See Exhibit A):

> **Is my personal information secure?**
> ClixSense utilizes the latest security and encryption techniques to ensure the security of your account information . . . . We view protection of users' privacy as a very important community principle. We understand clearly that you and your information are one of our most important assets.

8. Through at least 2016, Respondent did not utilize the latest security techniques in the following areas, as it promised to users in the statement described in Paragraph 7. Respondent failed to:

   a. perform vulnerability and penetration testing of the network;

   b. use techniques to protect the ClixSense website from commonly known or reasonably foreseeable vulnerabilities, and attacks from third parties attempting to obtain access to consumer information stored in Respondent's databases. For example, Respondent failed to:

      i. use Intrusion Detection and Prevention systems (IDPS), application-aware firewalls, or reverse proxies, among other techniques, to protect against Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Open Uniform Resource Locator (URL) redirection, and frameable clickjacking;

      ii. employ strong cryptographic algorithms and Transport Layer Security (TLS); and

      iii. use up-to-date Secure Sockets Layer (SSL) certificates;

   c. implement reasonable access controls. For example, Respondent failed to:

i. use segregation, among other techniques, to limit access between computers on ClixSense's network and between such computers and the Internet;

ii. utilize a password management solution, among other techniques, to prevent employees from storing plain text user credentials in personal email accounts, and on ClixSense's laptops; and

iii. change default login and password credentials for third-party company network resources;

d. implement techniques to detect anomalous activity and/or cybersecurity events. For example, Respondent failed to:

i. use logging to collect sufficient information to adequately assess cybersecurity events;

ii. implement an IDPS to alert Respondent of potentially unauthorized access to ClixSense's network; and

iii. use data loss prevention tools, among other techniques, to regularly monitor for unauthorized attempts to exfiltrate consumers' personal information across and outside ClixSense's network boundaries; and

e. use encryption, among other techniques, to prevent known risks to consumers' personal information, including consumers' names, addresses, email addresses, dates of birth, gender, answers to security questions, login and password credentials, and Social Security numbers, when stored in clear text, or otherwise unobfuscated, on ClixSense's network and devices.

9. Respondent's practices, as described in Paragraph 8, failed to meet the minimal data security measures prescribed by data security professionals since at least 2013. Those practices, therefore, were not the "latest security techniques" to secure consumers' personal information through at least 2016.

10. Since at least 2011, as described in Paragraph 8, Respondent stored consumers' personal information on ClixSense's networks in clear text, employing no encryption whatsoever to that data at rest. Respondent, therefore, did not utilize the latest encryption techniques to secure consumers' personal information through at least 2016, as it promised in the statement to users referenced in Paragraph 7.

RESPONDENT'S UNFAIR PRACTICES

11. Since 2010, Respondent has engaged in a number of unreasonable security practices that

led to the breach described in Paragraphs 13 to 20, which caused or are likely to cause substantial consumer injury. Among other things, Respondent:

a. failed to implement readily available security measures to limit access between computers on ClixSense's network, and between such computers and the Internet;

b. permitted employees to store plain text user credentials in personal email accounts, and on ClixSense's laptops;

c. failed to change default login and password credentials for third-party company network resources; and

d. maintained consumers' personal information, including consumers' names, addresses, email addresses, dates of birth, gender, answers to security questions, login and password credentials, and Social Security numbers, in clear text on ClixSense's network and devices.

12. Respondent could have addressed each of the failures described in Paragraph 11 by implementing readily available and relatively low-cost security measures.

13. In November 2015, a ClixSense user informed Respondent about a publicly available web browser extension that purportedly allowed users to automatically click on and view advertisements. The automated tool would potentially facilitate click fraud on Respondent, requiring Respondent to pay users for advertisements they did not view.

14. Without exercising precautions such as using a virtual machine to segregate the software from network credentials or users' personal information, Respondent downloaded the unknown and potentially harmful browser extension onto the ClixSense network in February 2016. Security experts have long opined that companies should have appropriate segregation between systems to avoid exposure of such information.

15. Following the downloading of the browser extension, and continuing for many months, one or more hackers used the browser extension as an entry point to obtain information to attack ClixSense's computer network. The hacker(s) then engaged in activities on ClixSense's network that put Respondent on notice that ClixSense's network had been compromised, including deleting content from the ClixSense website; accessing documents, email accounts, and credentials stored on employee laptops; changing employees' logins and passwords; redirecting email notifications for multiple network accounts, including ClixSense's cloud and Domain Name System (DNS) host services; and redirecting visitors to the ClixSense website to an unaffiliated adult-themed website.

16. On or about September 6, 2016, the hacker(s) used a set of credentials obtained from an email message on a compromised employee's company laptop to access an old server that Respondent no longer used and that Respondent should have disconnected from the

ClixSense network. These server credentials were the default credentials issued to ClixSense but never changed.

17. Because the old server was still connected to the ClixSense network, the hacker(s) was able to use it to connect to the active ClixSense server where consumer personal information was stored. The hacker(s) connected to ClixSense's active server and downloaded a copy of the ClixSense user table, which contained clear text information regarding 6.6 million consumers—including some 500,000 U.S. consumers.

18. Following this attack, the hacker(s) accessed and then published and offered for sale on a website known for posting of security exploits, personal information pertaining to approximately 2.7 million consumers, including full names and physical addresses, dates of birth, gender, answers to security questions, email addresses and passwords, as well as hundreds of Social Security numbers. The public availability of this data increases the likelihood of identity theft or fraud for consumers whose information was posted.

19. Misuse of the types of personal information ClixSense collects—including Social Security numbers, dates of birth, full names, physical addresses, gender, email addresses, usernames, passwords, and answers to security questions—is likely to facilitate identity theft, privacy harms, and other consumer injuries.

20. On September 11, 2016, Respondent published a data breach announcement on ClixSense's website. Two months later, on November 14, 2016, Respondent sent individual breach notification emails to U.S. consumers. Prior to these notifications, consumers had no way of independently knowing about Respondent's security failures and could not reasonably have avoided possible harms from such failures.

VIOLATIONS OF THE FTC ACT

Count I – Deception: Misrepresentation about Encryption

21. As described in Paragraph 7, in connection with the ClixSense website, Respondent has represented, directly or indirectly, expressly or by implication, that Respondent utilized the latest encryption techniques to ensure the security of users' personal information.

22. In fact, as set forth in Paragraphs 8 and 10, Respondent did not utilize any encryption techniques to ensure the security of users' personal information. Therefore, the representation set forth in Paragraph 21 is false or misleading.

Count II – Deception: Misrepresentation about Latest Security Techniques

23. As described in Paragraph 7, in connection with the ClixSense website, Respondent has represented, directly or indirectly, expressly or by implication, that Respondent utilized the latest security techniques to ensure the security of users' personal information.

24. In fact, in the as set forth in Paragraphs 8 to 9, Respondent did not utilize the latest security techniques to ensure the security of users' personal information. Therefore, the representation set forth in Paragraph 23 is false or misleading.

Count III – Unfairness: Failure to Employ Reasonable Security Practices

25. As described in Paragraphs 11 to 20, Respondent's failure to employ reasonable security practices 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.

26. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C § 45(a).

THEREFORE, the Federal Trade Commission this nineteenth day of June, 2019, has issued this complaint against Respondent.

By the Commission.

April J. Tabor
Acting Secretary

SEAL:
ISSUED: June 19, 2019