

Complaint

IN THE MATTER OF

JAMES V. GRAGO, JR.**D/B/A****CLIXSENSE.COM**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. C-4678; File No. 172 3003*
Complaint, June 19, 2019 – Decision, June 19, 2019

This consent order addresses James V. Grago, Jr.'s use of information security protocols for an online rewards website. The complaint alleges that Respondent has violated Section 5(a) of the Federal Trade Commission Act by failing to provide adequate security for consumer's personal information collected through his website. The consent order prohibits Respondent from false or deceptive statements regarding the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Personal Information, including the extent to which it utilizes (1) encryption techniques and (2) security techniques.

Participants

For the *Commission*: *Andrea Arias, Monique F. Einhorn, and Jamie Hine.*

For the *Respondents*: *Ryan Blaney, JB Kelly, and Bryan Mosca, Cozen O'Connor.*

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.

Complaint

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;

Complaint

- 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.

Complaint

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.

Complaint

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.

Complaint

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.

Decision and Order

Exhibit A


[Sign In](#) [Sign Up](#) [Toolbar](#) [Forum](#)

[View Ads](#) [Advertise](#) [ClixGrid](#) [My Account](#) [Affiliates](#) [Helpdesk](#)

[Home](#) > [Helpdesk](#) > [FAQ](#) > [General Information](#) > **Is my personal information secure?**  [Announcements](#) [My Tickets](#) [Submit a Ticket](#)

General Information

[When and how will I receive my earnings?](#)

[How do I earn money with ClixSense?](#)

[I received an email asking if I wanted to be a Mystery Shopper, is this legit?](#)

[I share a home with my brother, my cousin, and his girlfriend - Can we each have a ClixSense account?](#)

[Can I access my account from different locations?](#)

[My account is closed, can I reopen it?](#)

[How to update my profile information?](#)

[How do I close my account?](#)

[I can't see ad notifications in the toolbar or the toolbar has disappeared, what happened?](#)

 **Is my personal information secure?**

ClixSense utilizes the latest security and encryption techniques to ensure the security of your account information. We do not sell or rent your personal information to third parties for their marketing purposes. 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. ClixSense will however, always cooperate fully with law enforcement agencies and authorities in any investigations concerning fraud or any type of Internet crime. We store and process your information on computers located in the United States that are protected by physical as well as technological security devices.

Search FAQs

☒ Search only in General Information

Categories

- General Information**
- Premium Accounts
- Viewing Ads
- Advertising
- Affiliate Program

[About Us](#)
[User Agreement](#)
[Privacy Policy](#)
[Sitemap](#)

[View Ads](#)
[Advertise](#)
[Affiliates](#)
[Toolbar](#)

[Contact Us](#)
[Forum](#)
[FAQ](#)

[Follow Us](#)
[Facebook](#)






DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the

Decision and Order

Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: (1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits 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 Respondent has 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. Respondent is James V. Grago, Jr., individually and doing business as ClixSense.com, which is a sole proprietorship with its principal office or place of business in Hampstead, North Carolina.
2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

- A. “Covered Incident” means any instance in which any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- B. “Personal Information” means individually identifiable information from or about an individual consumer, including: (a) a first and last name; (b) a home or other physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other government-issued identification number; (g) a financial institution account number; (h) a credit or

Decision and Order

debit card number; (i) a photograph; (j) an authentication credential such as a login ID or password; and (k) an answer to a security question.

- C. “Respondent” means James V. Grago, Jr., individually and doing business as ClixSense.com, a sole proprietorship, and its successors and assigns.

Provisions**I. Prohibition Against Misrepresentations
About Privacy or Security of Personal Information**

IT IS ORDERED that Respondent, Respondent’s 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, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Personal Information, including the extent to which Respondent utilizes (1) encryption techniques; and (2) security techniques.

II. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, for any business that Respondent controls directly or indirectly, shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program (“Information Security Program”) that is designed to protect the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, Respondent must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;
- B. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- C. Assess and document, at least once every twelve months and promptly following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information;
- D. Design, implement, and document safeguards that address the internal and external risks Respondent identifies to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision II.C. Each safeguard shall take into account the sensitivity of Personal Information at issue;
- E. Assess, at least once every twelve months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the

Decision and Order

security, confidentiality, or integrity of Personal Information. Each such assessment must evaluate safeguards in each area of relevant operation, including: (1) employee training and management; (2) information systems, such as network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

- F. Test and monitor the effectiveness of the safeguards at least once every twelve months and promptly following a Covered Incident, and modify the Information Security Program based on the results;
- G. Select and retain service providers capable of safeguarding Personal Information they receive from Respondent, and contractually require service providers to implement and maintain safeguards for Personal Information; and
- H. Evaluate and adjust the Information Security Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve months.

III. Data Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Information Security Program, for any business that Respondent controls, directly or indirectly, that collects Personal Information online, Respondent must obtain initial and biennial assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who uses procedures and standards generally accepted in the profession. The Assessor preparing such Assessments must be: an individual qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); an individual holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.
- B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- C. Each Assessment must: (1) determine whether Respondent has implemented and maintained Provision II of this Order titled Mandated Information Security Program; (2) assess the effectiveness of Respondent's implementation and

Decision and Order

maintenance of sub-Provisions II.A-H; and (3) identify any gaps or weaknesses in the Information Security Program.

- D. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (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 Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re James V. Grago, Jr., d/b/a ClixSense.com, FTC File No.1723003." All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV. Prohibition Against Misrepresentations to the Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Data Security Assessments by a Third Party, must not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained Provision II of this Order titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-H; or (3) identification of any gaps or weaknesses in the Information Security Program.

V. Annual Certification

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Information Security Program, Respondent shall:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to

Decision and Order

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 James V. Grago, Jr., d/b/a ClixSense.com, FTC File No.1723003.”

VI. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order.
- B. For twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives with responsibilities related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in Provision VII of this Order titled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

VII. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which:
 1. 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 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; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of

Decision and Order

each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

2. Additionally, Respondent must: (a) identify all his telephone numbers and all his physical, postal, email and Internet addresses, including all residences; (b) identify all his business activities, including any business for which Respondent performs services whether as an employee or otherwise and any entity in which Respondent, individually, has any ownership interest; and (c) describe in detail Respondent's involvement in each such business activity, including title, role, responsibilities, participation, authority, control, and any ownership.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following:
1. Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of 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.
 2. Additionally, Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Respondent performs services whether as an employee or otherwise and (ii) any entity in which Respondent has any ownership interest and over which Respondent has direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (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

Decision and Order

Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.
The subject line must begin, "In re James V. Grago, Jr., d/b/a ClixSense.com,
FTC File No.1723003."

VIII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person providing services, 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. Copies or records of all consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;
- D. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, confidentiality, security, or integrity of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, confidentiality, security, or integrity of Personal Information, including the extent to which Respondent utilizes (1) encryption techniques; and (2) security techniques; and
- E. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

IX. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, 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 Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

Analysis to Aid Public Comment

- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, 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.

X. 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 twenty (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 twenty (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 twenty (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 terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from James V. Grago, Jr., individually and doing business as ClixSense.com ("Respondent").

Analysis to Aid Public Comment

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

This matter involves ClixSense.com (“ClixSense”), an online rewards website owned and operated by James V. Grago, Jr. (“Mr. Grago”) since 2010. As the sole owner of ClixSense, Mr. Grago controlled or had authority to control, or participated in the acts or practices alleged in the proposed complaint.

ClixSense pays its users for clicking on advertisements, performing online tasks, or completing online surveys. ClixSense makes money from advertisers and from marketers who purchase information generated from consumer surveys. As part of the enrollment process, ClixSense collects and stores personal information on its computer network about its users, including full names, physical addresses, dates of birth, gender, and email addresses. ClixSense also requires users to create a username, a password, and an answer to a security question that it stores in its database. For users who earn more than \$600 annually, ClixSense requires a Social Security number.

The Commission’s proposed three-count complaint alleges that Respondent has violated Section 5(a) of the Federal Trade Commission Act.

First, the proposed complaint alleges that Respondent deceived its users about the level of encryption it used. As alleged in the proposed complaint, Respondent has expressly represented to its users through a Frequently Asked Question (“FAQ”) entitled “Is my personal information secure?” that it uses the latest encryption techniques to ensure the security of account information. Contrary to this claim, the proposed complaint alleges that Respondent used no encryption to protect consumers’ personal information. In fact, Respondent stored consumers’ personal information, including SSNs, in clear text.

Second, the proposed complaint alleges that Respondent misrepresented to its users that it utilized the latest security techniques to ensure the security of users’ personal information. As alleged in the proposed complaint, Respondent failed to utilize the latest security techniques in multiple areas.

Third, the proposed complaint alleges that Respondent has engaged in a number of unreasonable security practices that led to a breach of information regarding 6.6 million consumers. The proposed complaint alleges that Respondent:

- failed to implement readily available security measures to limit access between computers on ClixSense’s network, and between such computers and the Internet;
- permitted employees to store plain text user credentials in personal email accounts, and on ClixSense’s laptops;

Analysis to Aid Public Comment

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

The proposed complaint alleges that Respondent could have addressed each of the failures described above by implementing readily available and relatively low-cost security measures.

The proposed complaint alleges that Respondent's failures 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. Such practice constitutes an unfair act or practice under Section 5 of the FTC Act.

The proposed order contains injunctive provisions addressing the alleged deceptive and unfair conduct in connection with Respondent's operation of an online rewards website. Part I of the proposed order prohibits Respondent from false or deceptive statements regarding the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Personal Information, including the extent to which it utilizes (1) encryption techniques and (2) security techniques.

Part II of the proposed order prohibits Respondent, in connection with any business that Mr. Grago controls directly and indirectly, including ClixSense, from transferring, selling, sharing, collecting, maintaining, or storing personal information unless it establishes and implements, and thereafter maintains, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of such personal information.

Part III of the proposed order requires any business that Mr. Grago controls, directly or indirectly, that collects personal information online to obtain initial and biennial data security assessments for twenty years.

Part IV of the agreement prohibits Respondent from misrepresenting any fact material to the assessments required by Provision III.

Part V requires any business that Mr. Grago controls directly or indirectly, including ClixSense, to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program) that Respondent has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Parts VI through IX of the proposed order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide

Analysis to Aid Public Comment

information or documents necessary for the Commission to monitor compliance. Part X states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

Complaint

IN THE MATTER OF

A WALDRON HVAC, LLC
D/B/A
WALDRON ELECTRIC HEATING AND COOLING, LLC,
AND
THOMAS J. WALDRON

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT AND SECTION 2 OF THE CONSUMER REVIEW FAIRNESS ACT

Docket No. C-4680; File No. 182 3077
Complaint, June 19, 2019 – Decision, June 19, 2019

This consent order addresses A Waldron HVAC, LLC's use of non-disparagement provisions in consumer form contracts in the course of selling their electrical, heating, and cooling services. The complaint alleges that the respondents violated Section 2(c) of the Consumer Review Fairness Act ("CRFA") by offering to consumers form contracts that contained non-disparagement provisions made void by Section 2(b) of the CRFA. The consent order prohibits, in the sale or leasing of any good or service, the respondents from: offering to any prospective customer a contract, or offering to any customer a renewal contract, that includes a review-limiting term; requiring that a customer accept such a term as a condition of the respondents' fulfillment of their obligations under contracts entered into before the effective date of the order; or attempting to enforce or assert the validity of such a term in customer contracts entered into before the effective date of the order.

Participants

For the *Commission*: Carl H. Settlemyer.

For the *Respondents*: Gregory A. Castelli, solo practitioner.

COMPLAINT

The Federal Trade Commission, having reason to believe that A Waldron HVAC, LLC and Thomas J. Waldron, individually and as an owner and manager of A Waldron HVAC, LLC (collectively, "Respondents"), have violated the Consumer Review Fairness Act of 2016, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent A Waldron HVAC, LLC (also d/b/a Waldron Electric Heating and Cooling, LLC) ("Waldron Electric") is a Pennsylvania limited liability company with its principal office or place of business at 500 Regis Avenue #18415, Pittsburgh, Pennsylvania 15236. Waldron Electric provides electrical, heating, and cooling services.
2. Respondent Thomas J. Waldron is an owner and manager of Waldron Electric. Individually or in concert with others, he controlled or participated in the acts and practices of Waldron Electric, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Waldron Electric.