[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 172 3003]

ClixSense.com; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement and Statement of the Commission.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order -- embodied in the consent agreement -- that would settle these allegations. The attached Statement of the Commission describes new requirements in recent data security orders.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write: "ClixSense.com; File No. 1723003" on your comment, and file your comment online at https://www.regulations.gov by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610

(Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Jamie Hine (202-326-2188), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR § 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for April 24, 2019), on the World Wide Web, at https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Write "ClixSense.com; File No. 1723003" on your comment. Your comment - including your name and your state - will be placed on the public record of this proceeding, including, to the extent practicable, on the https://www.regulations.gov website.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online through the https://www.regulations.gov website.

If you prefer to file your comment on paper, write "ClixSense.com; File No. 1723003" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at https://www.regulations.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential" – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website – as legally required by FTC Rule 4.9(b) – we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Proposed 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").

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;
- 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 are 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 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.

By direction of the Commission.

Julie A. Mack,
Acting Secretary.

Statement of the Federal Trade Commission

April 24, 2019

Today, the Commission announces cases against Clixsense and i-Dressup,[1] which include allegations that the companies failed to employ reasonable security to protect consumers' sensitive data. The orders obtained in these matters contain strong injunctive provisions, including new requirements that go beyond requirements from previous data security orders. For example, the orders include requirements that a senior officer provide annual certifications of compliance to the Commission, and explicit provisions prohibiting the defendants from making misrepresentations to the third parties conducting assessments of their data security programs. These new requirements will provide greater assurances that consumers' data will be protected going forward.

Since joining the Commission, we have instructed staff to closely review our orders to determine whether they could be strengthened and improved – particularly in the areas of privacy and data security. Through ongoing discussions both internally and with external stakeholders, including through our public *Hearings on Competition and Consumer Protection in the 21st Century* and the comment process,[2] we continue to consider changes to our orders. We will adjust our data security orders, as needed, to reflect our ongoing discussions regarding the FTC's remedial authority and needs, as well as the specific facts and circumstances of each case.

We are particularly committed to strengthening the order provisions regarding

---

[1] Although the Commission's settlement with i-Dressup addresses broader COPPA violations, this statement focuses specifically on the data security requirements set forth in the proposed stipulated order.

[2] *See, e.g.*, *FTC Hearings on Competition and Consumer Protection in the 21st Century* (Session 9 – Data Security), Dec. 11-12, 2018, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018.

data security assessments of companies by third parties. The Commission expects that these third parties will faithfully assess data security practices to identify potential noncompliance with appropriate order provisions. Future orders will better ensure that third-party assessors know they are accountable for providing meaningful, independent analysis of the data practices under examination. The announcements today reflect the beginning of our thinking, but we anticipate further refinements, and these orders may not reflect the approach that we intend to use in every data security enforcement action going forward.

[FR Doc. 2019-08786 Filed: 4/30/2019 8:45 am; Publication Date: 5/1/2019]