D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

MAY 2019

ADVERTISING, MARKETING & PROMOTIONS

>>ALERT

TWO WEBSITES SETTLE FTC ALLEGATIONS THAT THEY FAILED TO SECURE CONSUMER DATA

The Federal Trade Commission (FTC) recently announced settlements with operators of two websites claiming that the sites failed to take reasonable steps to protect consumer data, which resulted in the sites being accessed by hackers.

Significantly, these settlements contain new requirements beyond those mandated in previous data security cases, and indicate the FTC may be turning up the heat on its enforcement activities in this area.

I-DRESSUP SETTLEMENT

In the first action, the FTC claimed that Unixiz, Inc. dba i-Dressup.com (i-Dressup) and its chief executive officer violated the Children's Online Privacy Protection Act (COPPA) by failing to obtain parental consent before collecting personal information from children under 13 years of age and by not providing reasonable and appropriate security for the data it collected from its users.

According to the FTC, the i-Dressup website, which allows its members — including children — to play dress-up games, design clothes and decorate their space and includes an online community where members could create personal profiles and interact with each other, required members to submit a username, password, birthdate and email address to register for the site. If a prospective member indicated that he or she was over 13 years of age, the member had access to all of the features of the site. If a prospective member's registration indicated that he or she was under 13 years of age, i-Dressup would request a parent's email address to send the parent a consent request. If the parent did not consent, children under 13 could participate in a "Safe Mode" membership with limited access to the site's games and features. However, even in instances where the parent did not consent to the child's use of the site, i-Dressup collected and retained the personal information provided by the child during registration, and did not delete such information.

The FTC further claimed that i-Dressup violated COPPA's requirement to keep the data it collected reasonably secure. The FTC contended that the company engaged in a number of practices that, taken together, failed to reasonably and appropriately secure and protect personal information and other data collected from consumers, including children. Among i-Dressup's concerning activities was its practice of storing and transmitting consumer personal information in plain text. The FTC also claimed that the site failed to perform vulnerability testing on its network, implement an intrusion detection and prevention system and

>> continues on next page

THE BOTTOM LINE

The security of consumer data is an important priority for the FTC and has become even more important in recent years, particularly when such data is subject to attacks by malicious third parties. The FTC emphasized that both settlements contained "new requirements" going beyond requirements from previous data security orders.

Perhaps even more importantly, the FTC's statement indicated that the agency has instructed staff to closely review its orders to determine whether they can be strengthened and improved, "particularly in the areas of privacy and data security" and particularly with respect to "data security assessments of companies by third parties." This suggests that the FTC is likely to continue to bring such actions going forward — and may seek stronger penalties than it has in the past.

monitor for potential security incidents. i-Dressup's failures reportedly led to a security breach whereby a hacker accessed the personal information of 2.1 million users, including that of approximately 245,000 children under 13 years of age.

Pursuant to the FTC's settlement, i-Dressup agreed to pay $35,000 in civil penalties and is:

1) Barred from sharing or collecting any personal information until it implements a comprehensive data security program to protect its users' personal information;

2) Prohibited from making misleading statements to the third-party auditors assessing their data security programs; and

3) Is subject to independent biennial assessments of its new security program and must provide an annual certification of compliance to the FTC.

CLIXSENSE SETTLEMENT

In the second action, the FTC claimed that ClixSense.com (ClixSense), an online rewards site that pays users to view ads, complete online surveys and perform online tasks, did not maintain adequate data security mechanisms to protect consumer personal information in violation of Section 5 of the FTC Act.

According to the FTC, the website collected personal information from users, which it promised to protect by using "the latest security and encryption techniques." The FTC found that such promises were false and intentionally deceptive, as ClixSense had not even implemented minimal security measures. For instance, it stored consumer personal information in plain text with no encryption. Additionally, the company did not perform vulnerability and penetration testing of the network or implement reasonable access controls, nor did it 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 ClixSense's databases. In the FTC's opinion, ClixSense's practices failed to meet the minimal data security measures prescribed by data security professionals since at least 2013.

The FTC also alleged that ClixSense's lack of security allowed hackers to gain access to its network using ClixSense's browser extension as an entry point. The hackers ultimately downloaded a copy of the ClixSense user table, which contained plain text information regarding 6.6 million consumers — including about 500,000 U.S. consumers. The hackers published and offered for sale these consumers' personal information, including full names, physical addresses, answers to security questions, passwords and hundreds of Social Security numbers.

The FTC's settlement with ClixSense and its sole proprietor James V. Grago, Jr.:

1) Prohibits Grago from making misrepresentations in the future about privacy or the security of personal information for any company he controls;

2) Mandates that Grago undertake an information security program for any business that he controls;

3) Requires Grago to obtain biennial third-party data security assessments by an independent third party; and

4) Requires Grago to provide an annual certification of compliance to the FTC.

FOR MORE INFORMATION

Allison Fitzpatrick
Partner
212.468.4866
afitzpatrick@dglaw.com

Vivian Byrwa
Associate
212.468.4927
vbyrwa@dglaw.com

Samantha G. Rothaus
Associate
212.468.4868
srothaus@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com