hopkins carley

[redacted]

November 22, 2021

[redacted]

***Via E-Mail***

Cooper Barry deNicola [redacted]
Miles McCain [redacted]
Aditya Saligrama [redacted]

***Re: Buzz Vulnerability Disclosure***

To: Cooper de Nicola, Miles McCain and Aditya Saligrama

Hopkins & Carley represents The Buzz Media Corp. ("Buzz"). We write regarding your team of security researchers, both individually and collectively (referred to herein as the "Group") to make you aware of the Group's criminal and civil liability arising out of the Group's unauthorized access to Buzz's systems and databases.

Based on your own admissions in your email dated November 9, 2021 notifying Buzz of the security vulnerability, the Group explored "…*the vulnerability*…" and obtained unauthorized access to Buzz's "…*complete databases*…" and all information stored in Buzz's database. Your email further goes on to state that the Group edited user tables and created moderator and administrator accounts enabling the Group to access Buzz's systems without authorization.

The Group's actions in obtaining this unauthorized access to Buzz's databases violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (CFAA), the Digital Millennium Copyright Act (DMCA) and Buzz's Terms of Use.

The Group circumvented Buzz's technological measures designed to protect Buzz's databases, without any permission or authority in violation of the DMCA. For these violations of the DMCA the Group may be liable for fines, damages and each individual of the Group may be imprisoned. Further, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (CFAA) imposes additional criminal and civil liability for unauthorized access to a protected computer, including accessing files or databases to which one is not authorized to access. The CFAA prohibits intentionally accessing a protected computer, without authorization or by exceeding authorized access, and obtaining information from a protected computer. Criminal penalties under the CFAA can be up to 20 years depending on circumstances.

Buzz's own Terms of Use expressly prohibits any of the following actions and clearly sets forth that the Group has no authorization to access Buzz's systems or databases "…*attempt to reverse engineer any aspect of the Services or do anything that might circumvent measures employed to prevent or limit access to any area, content or code of the Services (except as otherwise expressly permitted by law); Use or attempt to use another's account without authorization from such user and Buzz; Use any automated means or interface not provided by Buzz to access the Services;*…" Not only then are the Group's actions a violation of both the DMCA and the CFAA, as indicated above, the Group's actions are also a violation of Buzz's Terms of Use and constitute a breach of contract, entitling Buzz to compensatory damages and damages for lost revenue.

Notably, under the CFAA, the Group's agreement to infiltrate Buzz's network is also a separate offense of conspiracy, exposing the Group to even more significant criminal liability.

The Group should also take note of the Stanford Computer and Network Usage Policy available at https://adminguide.stanford.edu/chapter-6/subchapter-2/policy-6-2-1. We draw your attention to Section 2(b) of such Policy which prohibits the following: "*Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person's information are a violation of University policy and may also violate applicable law, potentially subjecting the user to both civil and criminal liability*." In conducting the Group's research, we have reason to believe that the Group used Stanford's network in violation of this Policy. Indeed, your email of November 9, 2021 was sent using the Stanford network and email domains in violation of this Policy.

While Buzz thanks you for the information regarding the security vulnerability, Buzz does not condone the Group's actions or encourage such actions. We trust that the Group was well intentioned in trying to help Buzz. Therefore, we demand that each Group member confirm their agreement to maintain confidentiality of this matter and all information regarding the security vulnerability. Each member of the Group must reply via email to confirm that the Group will: cease engaging in this conduct to access any portion of the Buzz systems or databases; destroy any and all information or data obtained through access to Buzz's networks and databases; and will not use, publicize or disclose any information regarding the security vulnerability or information from Buzz's networks or databases. Provided that we receive your confirmation within five (5) days of the date of this letter, Buzz will not pursue charges against the Group.

Buzz reserves all of its rights and remedies, at law and in equity. Please direct all further communications regarding this matter to my attention.

Sincerely,

HOPKINS & CARLEY
A Law Corporation

[redacted]

Copy to:

Ashton Cameron Cofer [redacted]
Edward Gabriel Solomon [redacted]