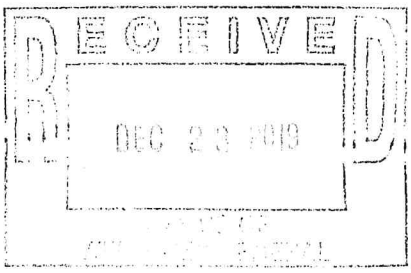
HOGE · FENTON

ATTORNEYS

Stephanie O. Sparks
408.947.2431
stephanie.sparks@hogefenton.com

December 20, 2019

Via First Class U.S. Mail



The Honorable Wayne Stenehjem
Attorney General of North Dakota
North Dakota Attorney General's Office
600 E. Boulevard Ave, Dept. 125
Bismarck, ND 58505

Re: ToonDoo.com Data Breach

Dear Attorney General Stenehjem:

I write on behalf of Jambav, Inc. ("Jambav"), a Delaware corporation, that had a comic strip creation tool referred to as "ToonDoo" available online at ToonDoo.com. On or about November 11, 2019 2:30 a.m. EST, Jambav noticed Twitter content stating that the ToonDoo.com website had been hacked and the personal information of ToonDoo users had been compromised.

Within two hours of learning that the ToonDoo.com website may have been hacked, Jambav immediately shut down the website. The following day, Jambav discovered that Toondoo.com accounts had been compromised, however Jambav is unable to determine how the breach occurred or its extent. An independent cybersecurity firm is being engaged to conduct a forensic investigation to determine the nature and scope of the incident, including which account(s) and which data may have been compromised.

At the time Jambav shut down the website, there were approximately 6.1 million users who had ToonDoo.com accounts. To set up accounts, ToonDoo users provided their usernames, passwords, email address and gender. In some instances, sign up IP addresses and thus location information were also collected. Of these total users, Jambav believes that approximately 2,699,637 users are in the United States and U.S. territories. Jambav believes the approximate number of potentially impacted residents of the State of North Dakota is 8,850.

193220

Jambav has reported this crime to the Federal Bureau of Investigation's Internet Crime Complaint Center and will fully cooperate with any law enforcement activities. An independent cybersecurity firm is being engaged to conduct a forensic investigation to determine the nature and scope of the incident, including the specific data impacted.

Jambav is in the process of directly notifying all potentially impacted ToonDoo users of the breach via their email addresses (a copy of the individual notification is enclosed), and it has posted notice on its ToonDoo.com website. Both email notifications and the website posting will provide consumers information about the incident, steps they can take to protect themselves against the potential misuse of their information, and an email address (support@toondoo.com) and toll free phone number (+1 (800) 299-4101) through which they can contact Jambav Monday through Friday, 8:30 a.m. to 5:00 p.m. Central Time to obtain further information.

Please do not hesitate to contact me if you have any questions regarding this notification.

Very truly yours,

HOGE, FENTON, JONES & APPEL, INC.

Stephanie O. Sparks

Stephanie O. Sparks

SOS:tw

Encls.

JAMBAV, INC.

Date: [Insert Date of notice]

NOTICE OF DATA BREACH

Dear **[Insert Email Address]**,

We are contacting you about a data breach of the website at www.ToonDoo.com ("ToonDoo").

The password used by you for the Toondoo account has been compromised. If you have used the same password for other purposes, you must change the password in such other places.

What Happened?

On November 11, 2019, we became aware that there has been a data breach at Toondoo.com. We immediately shut down the Toondoo website.

What Information Was Involved?

ToonDoo users' email addresses, usernames, passwords, and gender, and in a few instances, the Internet Protocol (IP) address from which users signed up for a ToonDoo account and hence such users' geographic location, namely, city and U.S. state or country, as the case may be. ToonDoo did not have any credit card or other financial information, U.S. Social Security numbers, or other highly sensitive personal information.

What We Are Doing

On November 11, 2019, as soon as we discovered that ToonDoo user information had been compromised, JAMBAV, Inc. immediately shut down the website. An independent forensics company to investigate the nature and extent of the breach is in the process to be engaged. We have filed a complaint with the U.S. Federal Bureau of Investigation ("FBI"), are otherwise engaging with law enforcement authorities, and will cooperate and assist in any of their investigation activities.

What You Can Do

Even though ToonDoo had no financial information, U.S. social security numbers and other similarly highly sensitive personal information, we strongly recommend that you be proactive in protecting yourself from possible fraud, identity theft or other illegal activity using your personal information. You can follow the recommendations in the next section to protect your personal information.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your U.S. state attorney general, and/or the U.S. Federal Trade Commission ("FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major U.S. credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three U.S. national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. You can continue to renew your fraud alert. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three U.S. national credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	**Maryland Attorney General** 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	**North Carolina Attorney General** 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	**Rhode Island Attorney General** 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400

If your personal information has been misused, visit the U.S. Federal Trade Commission's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the U.S. Federal Trade Commission's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

For More Information

We take your protection seriously and sincerely apologize for the inconvenience this incident may cause you. If you have questions or need assistance, call +1 (800) 299-4101, between 8:00 a.m. to 5:00 p.m. Central Time, Monday through Friday. Or you can write to us at **support@toondoo.com**.

JAMBAV, INC.

1000 Northwest Street, Suite 1200
Wilmington, Delaware 19801 USA

Office of Attorney General
RECEIVED

DEC 27 2019

Consumer Protection
Bismarck North Dakota