HOGE · FENTON
ATTORNEYS

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

January 2, 2020

Via E-Mail and First Class U.S. Mail

The Honorable Kathy Jennings
Attorney General of Delaware
Delaware Department of Justice
Consumer Protection Unit
820 N. French Street, 5th Floor
Wilmington, DE 19801

Email: security.breach.notification@state.de.us

Re: ToonDoo.com Data Breach

Dear Attorney General Jennings:

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. Enclosed with this letter is a copy of Jambav's responses to Delaware's online Security Breach Notification Form. 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. All passwords were stored using MD5 hashing with unique per user salt. 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 Delaware is 6,382.

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. Delaware residents were notified by email on December 15, 2019 EST. 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

Encl.

MODEL DATA SECURITY BREACH NOTIFICATION FORM

Notice to the Delaware Attorney General

Delaware Department of Justice
Consumer Protection Unit
820 N. French Street, 5th Floor
Wilmington, DE 19801
security.breach.notification@state.de.us

The Consumer Protection Unit of the Delaware Department of Justice is making this Model Data Security Breach Notification Form available to provide assistance and guidance to businesses and other entities who are subject to Delaware's data breach notification law and are required to give notice of a data breach to the Attorney General under Title 6, § 12B-102(d) of the Delaware Code.

The Consumer Protection Unit will deem use of this Model Data Security Breach Notification Form to constitute appropriate written notice to the Attorney General that is required under Title 6, § 12B-102(d) of the Delaware Code. Other forms of written or electronic notice may be appropriate, but must provide the same information sought by this form.

Do not use this form to provide the notice to consumers and other affected persons required under Title 6, § 12B-102(a) of the Delaware Code. A model form for that purpose is available on the Consumer Protection Unit's security breach notification webpage:

https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification

PLEASE NOTE: The information disclosed on this form, or otherwise provided to the Department of Justice pursuant to Title 6, § 12B-102(d) of the Delaware Code, may constitute a public record subject to disclosure under Delaware's Freedom of Information Act (Title 29, Chapter 100) ("FOIA"). FOIA requires that the Department of Justice's records are public records (unless otherwise declared by FOIA or other law to be exempt from disclosure) and are subject to inspection and copying by any person upon a written request. A person providing notice of a security breach to the Department of Justice may request confidential treatment when it delivers the notice, by identifying the information for which confidential treatment is sought, representing in good faith that the information is not a "public record" as defined in FOIA, and briefly stating the reason(s) why. The Department of Justice will independently determine the validity of the request for confidential treatment.

SECURITY BREACH NOTIFICATION FORM

Delaware Department of Justice
Consumer Protection Unit
820 N. French Street
Wilmington, DE 19801
security.breach.notification@state.de.us

Type of Report
◉ Initial Breach Report
○ Addendum to Previous Report

Entity That Owns or Licenses the Computerized Data Whose Security Was Breached					
Name:	Jambav, Inc., a Delaware corporation				
Street Address:	1000 N. West Street, Suite 1200				
City:	Wilmington	State:	DE	ZIP Code:	19801

Submitted By					
Name:	Stephanie O. Sparks	Title:	Shareholder		
Firm (*if different*):	Hoge, Fenton, Jones & Appel, Inc.				
Street Address:	60 South Market Street, Suite 1400				
City:	San Jose	State:	CA	ZIP Code:	95113
Telephone:	408-947-2431	Email:	stephanie.sparks@hogefenton.com		
Relationship to Entity That Was Breached:	Outside legal counsel				

Type of Organization

☐ Charitable/Non-Profit	☐ Educational	☐ Financial Services
☐ Government – Delaware	☐ Government – Outside Delaware	☐ Healthcare
☐ Insurance	☐ Retail/Merchant	☐ Utility

■ Other (please describe): Service provider of online games; released ToonDoo, an online comic strip creating tool, in 2007.

Type of Personal Information Involved in the Security Breach

Delaware resident's first name or first initial and last name, in combination with 1 or more of the following (mark all that apply):

☐ Social Security number	☐ Driver's license number
☐ Federal identification card number	☐ Passport number
☐ Individual taxpayer ID number	☐ Biometric data
☐ Deoxyribonucleic (DNA) profile	☐ Medical history
☐ Medical treatment by a healthcare professional	☐ Diagnosis of mental/physical condition by healthcare professional

☐ Health insurance policy number, subscriber ID number, or any other unique identifier used by health insurer to identify person

☐ Account number, credit card account number, or debit card number, in combination with any required security code, access code, or password that would permit access to a financial account

■ Username or email address, in combination with password or security question and answer to access online account

Number of Persons Affected	
Delaware Residents Only	approx. 6,382
Total (*including Delaware*)	approx. 6.1 million

Dates	
Breach(es) Occurred (*include start/end dates if known*)	Unknown
Breach(es) Discovered	November 11, 2019
Consumers Notified	December 15, 2019

Form of Notice to Affected Persons*	
☐ Written	☐ Telephonic
■ Electronic	☐ Substitute Notice

** Please attach a sample of the notice*

Was Notification Delayed Because of Law Enforcement Request?	
○ Yes	◉ No

Type of Security Breach (*mark all that apply*)

- ☐ Loss or theft of device or media
- ☐ Internal system breach
- ☐ Insider wrongdoing
- ■ External breach (*hacking, malware, etc.*)
- ☐ Payment card fraud
- ☐ Inadvertent disclosure
- ☐ Improper disposal
- ☐ Other (*please describe*): _____

Was Information Encrypted?

○ Yes ◉ No

Was Encryption Key Acquired?

○ Yes ○ No ◉ N/A

Brief Description of the Security Breach

On or about November 11, 2019 2:30am EST, Jambav noticed Twitter content stating ToonDoo.com website had been hacked & personal information of ToonDoo users had been compromised. Within 2 hours, Jambav shut down website. 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 scope of the incident, including which account(s) and which data may have been compromised. ToonDoo users provided their usernames, passwords,email addresses and gender and, in some instances, sign up IP addresses and thus location information was collected. All passwords were stored using MD5 hashing with unique per user salt.

Location of Breached Information

- ☐ Desktop computer
- ☐ Portable/Laptop computer
- ☐ Smartphone
- ☐ Network server
- ■ Cloud-Based Server
- ☐ Email
- ☐ Other (*please describe*): _____

Actions Taken in Response to the Security Breach (*mark all that apply*)

- ☐ Added/strengthened data encryption
- ☐ Changed password/strengthened password requirements
- ☐ Created/updated formal written information security plan
- ☐ Implemented new technical safeguards
- ☐ Improved physical security
- ☐ Revised policies and procedures
- ☐ Sanctioned workforce members involved (incl. termination)
- ☐ Trained or retrained workforce members
- ☐ Implemented periodic technical and nontechnical evaluations/risk analyses/penetration tests
- ☐ Revised contracts with business partners, vendors, subcontractors, service providers
- ☐ Changed business partners, vendors, subcontractors, service providers
- ■ Other (*please describe*): Shut down website

Credit Monitoring or Identity Theft Protection Services Offered?

☐ Credit monitoring ☐ Identity theft protection	Duration:	N/A
	Provider:	N/A
Briefly describe services:	N/A	

Law Enforcement Agency Notified of Security Breach?

◉ Yes
○ No

Name of Agency:	Federal Bureau of Investigation Internet Crime Complaint Center
Contact Name and Number:	None given by FBI
Report Number (*if applicable*):	N/A

Submit Form

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

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