Clark Hill

M. Scott Koller
T (213) 226-4736
F (312)985-5952
Email:skoller@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

November 20, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

We represent DanceBUG Inc. ("DanceBUG") with respect to a data security incident involving personal information as described below. DanceBUG takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

After reports of fraudulent charges on payment cards used legitimately on the DanceBUG website, DanceBUG engaged a cybersecurity firm to investigate. On October 10, 2024, the investigation revealed that an unauthorized person gained access to the server hosting the website. The attacker installed a malicious program designed to record information entered by customers. Based on the investigation, DanceBUG believes information entered on the website from April 2024 to August 2024 could have been accessed, which includes names, addresses, payment card numbers, expiration dates, and verification codes.

2. Number of Maryland residents affected

Fifty-four (54) residents of Maryland were notified of the incident. Notification letters were sent to potentially affected individuals on November 20, 2024. A copy of the template notification letter is attached as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, DanceBUG has completely eradicated the malware from its systems and has been working with cyber security firms to further strengthen its security measures. Additionally, DanceBUG has implemented enhanced monitoring and preventative measures to safeguard against future threats. Additionally, affected individuals were offered twelve (12) months of credit monitoring and identity protection services through TransUnion.

4. Contact information

DanceBUG takes the security of the information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at skoller@clarkhill.com or (310) 928-7524.

Sincerely,

CLARK HILL

M. Scott Koller
Member

cc: Sunaina Ramesh

DanceBUG Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Exhibit A

[redacted]

000010102G0500
P

November 20, 2024

NOTICE OF DATA SECURITY INCIDENT

Dear [redacted]

DanceBUG Inc. is writing to inform you of a security incident involving some of your information. This letter explains the incident, the measures we have taken, and some steps you may consider taking.

What Happened?
After reports of fraudulent charges on payment cards used legitimately on our website, we engaged a cybersecurity firm to investigate. On October 10, 2024, the investigation revealed that an unauthorized person gained access to the server hosting our website. The attacker installed a malicious program designed to record information entered by customers. Based on our investigation, we believe information entered on our website from April 2024 to August 2024 could have been affected.

What Information Was Involved?
The affected information may include your name, address, payment card number, expiration date, and verification code. Our records indicate that you made a purchase using a payment card ending in [redacted] during the affected time period.

What We Are Doing:
We have since completely eradicated the malware from our systems and have been working with cyber security firms to further strengthen our security measures. Additionally, we have implemented enhanced monitoring and preventative measures to safeguard against future threats. In addition, we are offering you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your TransUnion credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. With this protection, TransUnion will help you resolve issues if your identity is compromised.

What You Can Do:
To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized activity to your financial institution because the major credit card companies have policies to prevent cardholders from being responsible for fraudulent charges.

For More Information:
We deeply regret any inconvenience this may cause and remain committed to safeguarding your information. If you have questions, please call [redacted] Monday through Friday from 8:00 am to 8:00 pm Eastern Time, excluding holidays.

Sincerely,
DanceBUG Inc.

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. To enroll in Credit Monitoring services at no charge, please log on to **https://benefit.identityforce.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

P 0000102028000

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 27 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.