LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

August 29, 2018

VIA ELECTRONIC SUBMISSION

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-Mail: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent LÍLLÉbaby in connection with a recent data security incident which is described in greater detail below. LÍLLÉbaby takes the privacy and security of the information within its control very seriously and is taking steps to help prevent a similar incident from occurring in the future.

1. Nature of the data security incident.

In June of 2018, LÍLLÉbaby learned of a potential data security incident involving the unauthorized installation of malware on the LÍLLÉbaby e-commerce web platform. As soon as LÍLLÉbaby discovered the incident, LÍLLÉbaby took immediate steps to secure payment card information belonging to LÍLLÉbaby customers. LÍLLÉbaby also launched an investigation and retained a leading forensics firm to determine what happened and whether customer payment card information had been accessed or acquired without authorization. In addition, LÍLLÉbaby reported the matter to the Federal Bureau of Investigation ("FBI") as well as to the payment card brands in order to help protect customer payment card information and to help prevent fraudulent activity.

It appears that payment card information including names, payment card numbers, expiration dates, and security codes may have been affected for customers who utilized the LÍLLÉbaby website from June 2016 until July 9, 2018.

2. Number of Washington residents affected.

LÍLLÉbaby has identified 1,557 Washington residents who may have been impacted by this incident. Notification letters were mailed to all affected individuals on August 28, 2018. A sample copy of the letter provided to potentially impacted individuals is included with this letter.

3. Steps taken relating to the incident.

LÍLLÉbaby has taken significant affirmative steps to help prevent a similar situation from arising in the future and to protect the privacy and security of all sensitive information in its possession. These steps have included working with a leading forensics firm to remove malicious code from the LÍLLÉbaby e-commerce web platform. LÍLLÉbaby has also taken steps to increase the security of its e-commerce platform (Magento) and has transitioned to processing payment cards through Payflow Pro IFrame to bolster transaction security. LÍLLÉbaby is now in the process of rebuilding its web platform in order to enhance the security of its payment card environment.

4. Contact information.

LÍLLÉbaby is committed to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052, or by e-mail at Alyssa.Watzman@lewisbrisbois.com.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

C/O ID Experts
PO Box 10444
Dublin, OH 43017-4044

To Enroll, Please Call:
(855) 474-3901
Or Visit:
https://ide.myidcare.com/LILLEbaby
Enrollment Code:
<<XXXXXXXX>>

<<Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>

August 28, 2018

Subject: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We at LÍLLÉbaby are writing to inform you of a data security incident that may have affected your payment card information. We view all of our customers as part of our family and we take the privacy and security of your information very seriously. We sincerely apologize for any concern that this incident may cause and are sending this letter to inform you about the steps you can take to help protect your information.

What Happened? In June of 2018, we learned of a potential data security incident involving the unauthorized installation of malware by a third party on our e-commerce web platform. As soon as we discovered the incident, we took immediate steps to secure payment card information belonging to our customers. We also launched an investigation and retained a leading forensics firm to determine what happened and whether customer payment card information had been accessed or acquired without authorization.

What Information Was Involved? We believe that malware installed on our e-commerce web platform by a third party could have comprised payment card information belonging to customers who purchased products from June 2016 to July 9, 2018. The affected information may have included names, payment card numbers, expiration dates, and security codes. No other personal information (for example, Social Security number and/or date of birth) was impacted.

What Are We Doing? Upon discovering this incident, we took the steps described above. We also reported the incident to the Federal Bureau of Investigation ("FBI") and will provide whatever cooperation is necessary to hold the perpetrators accountable. In addition, we reported the matter to the payment card brands in order to help protect your payment card information and to help prevent fraudulent activity. We are also providing you with information about steps that you can take to help protect your personal information and are offering you identity monitoring services for twelve (12) months at no cost to you. Finally, we have taken steps to enhance the security of customer information and our e-commerce web platform in order to help prevent similar incidents from occurring in the future.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

As an added precaution, we have arranged to have ID Experts help protect your identity for twelve (12) months at no cost to you. The services provided by ID Experts include Cyberscan Dark Web Monitoring, $1,000,000 of identity theft reimbursement insurance, and unlimited access to the ID Experts team. To enroll in these services, please call (855) 474-3901 or visit https://ide.myidcare.com/LILLEbaby. The deadline to enroll in these services is November 28, 2018.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions please call ID Experts at (855) 474-3901 from 5 am – 5 pm Pacific Time, Monday through Friday.

Thank you for your loyalty and your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Jeff Colton, CEO
LÍLLÉbaby

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 and review 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 should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major 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, GA 30348. You can also contact one of the following three 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	www.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. 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 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, the FTC 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 FTC 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.