PRINCESS POLLY

[Date]

[Individual Name]
[Individual Address]

RE: Notice of Data Breach

Dear [Individual Name],

We are contacting you to let you know of a recent security incident with our website. This notification explains what happened, how it may impact you and it sets out steps you can take in response, should you feel it necessary to do so.

What Happened? On or around April 24, 2019, Princess Polly Online Pty Ltd ("Princess Polly") was notified of suspicious activity related to certain credit cards used in transactions on its Australian website www.princesspolly.com. Princess Polly immediately launched an investigation into this report. Through this investigation, Princess Polly determined that an unidentified third party recently gained unauthorized access to our website. During this process, the third party may have accessed your personal information and payment details entered at check-out between November 1, 2018 and April 29, 2019.

The Princess Polly US website – us.princesspolly.com was not affected by this incident.

As soon as we became aware of this incident, we took immediate steps to investigate and confirm that our website was secure. We have appointed external IT and Cyber Security consultants to fully investigate this incident. These experts have confirmed that our website is secure, including any personal or payment information provided when shopping with Princess Polly.

We have been working closely with leading external IT and Cyber Security consultants to confirm which customers may have been impacted and identify precisely which information is involved in the incident.

The credit/debit card information of customers using Afterpay or PayPal has not been affected.

What Information Was Involved? The personal information which could have been impacted by the incident may include some or all of the following categories of information (if provided by you):

- billing and shipping name, address, email and phone number;
- the credit/debit card details you provided to complete the purchase;
- your date of birth; and
- your Princess Polly username and password.

We confirm that no other information about you was impacted by this incident. For those customers who made purchases using Afterpay or PayPal, your payment information has not been affected.

What We are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of this incident, we took steps to secure our e-commerce site and to find

out what happened. Additionally, as part of our ongoing commitment to the security of the customer information in our care, we have further strengthened our security measures. Our external IT and Cyber Security specialists confirmed our system is secure and we upgraded our credit card provider to Braintree, a PayPal owned company, who meet the highest security standards. Our U.S. website us.princesspolly.com was not affected by this incident.

What You Can Do. You may review the enclosed "Steps You can Take to Prevent Identity Theft and Fraud" to learn more about how to better protect against fraud and identity theft. We encourage you to review your credit/debit card statements and report any suspicious charges to the issuer of your card. Additionally, as Princess Polly accounts may have been impacted, we recommend changing all passwords that may have been identical or similar to the password used to access your Princess Polly account.

For More Information. If you have any further questions about this notification, please visit our website for more information: www.princesspolly.com/security-incident, email us at privacy@princesspolly.com.au, or call our dedicated assistance line at 1-855-644-2743, Monday through Friday from 6:00 am - 6:00 pm and Saturday and Sunday from 8:00 am – 5:00 pm PST.

We are extremely sorry that this incident has occurred. At Princess Polly, we have always prided ourselves on doing the best we can for our customers and apologize for any impact this incident has on our customers. We take the protection of our customers' data very seriously and have further strengthened our security measures to ensure that our customers' information is secure.

Kind regards,

Wez Bryett
Co-CEO
Princess Polly Online Pty Ltd

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended

fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For 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 violators. 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. We encourage you to 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.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 747 Rhode Island residents impacted by this incident