NOTICE OF DATA BREACH

I have lousy news to share: some time between May 1st and May 16th, the Black Phoenix Alchemy Lab site was hacked. [This does not apply to Trading Post or TAL; it was only BPAL's main site that was affected.] There is no way for our dev team to be absolutely certain when the attack initially happened, so this is the best educated guess based on the information we have. This is the first time that our data has been breached in the sixteen years that we've been in business. We take our customers' privacy, confidentiality, and security extremely seriously, and we are devastated that this incident occurred.

Yesterday, we learned from our devs that all passwords on the site needed to be changed. At the time, we didn't have further details but took immediate steps to learn what was going on, and the moment that the malicious code was discovered, our devs neutralized it.

I didn't want to post more until we understood exactly what happened. Although we cannot be sure that any of your information was accessed or misappropriated, we want to make you aware of the situation and provide you with information on what to do from here. So, here's what we know as of today -

WHAT HAPPENED

Malicious code was injected into the portion of the checkout page where credit card info bound for AuthorizeNet is gathered. If you made a purchase using the AuthorizeNet gateway during this period, your credit card data may have been compromised. We do not store any credit card info ourselves on the site – none whatsoever - so there was no credit card data to harvest from before this time period.

Any purchases made through the PayPal gateway were not affected. Any sales made in-person at a convention were not affected, nor were any purchases made through BPTP, TAL, our Amazon store, or our etsy shop.

On May 16th, our developer found this malicious code, but didn't immediately know what it was about. We immediately initiated the sitewide password reset to be safe while the developer tried to suss out what was going on. Most of the day was spent analyzing the code, and based on the information we now have, our developer determined that the malicious code was inserted for the purposes of harvesting credit card numbers.

Once that was established, I started drafting this announcement while Black Phoenix and our developers continued to research the situation.

It looks like less than 150 credit card transactions were at risk, and we will do everything in our power to directly contact anyone that might have been compromised.

WHAT INFORMATION WAS INVOLVED

The credit card numbers of under 150 customers who made purchases on the site using the AuthorizeNet gateway have possibly been compromised.

We do not know if any other data was accessed, as a bogus admin account was created by the person(s) who created the breach. Information that could have been accessed without authorization could have included your name, credit card billing address, telephone number, email address, and credit card

number data, the name on card, expiration date, and security code.

WHAT WE ARE DOING

We take our obligation to safeguard your information very, very seriously, and we did all that was within our power to act as quickly as possible. A bulk password reset was initiated as soon as malicious activity was suspected. As soon as the malicious code was found, our developers neutralized it. A full security audit was performed. We moved the entirety of the site to a new server with a managed infrastructure for added security. When the fake admin account was found, it was removed. Our developer is in the process of further hardening our security to ensure that breaches do not occur in the future and initiating a more robust intrusion detection system, and we are in the process of directly contacting the 150ish people whose credit card numbers may have been compromised. We are also notifying AuthorizeNet, the FBI, and local law enforcement in Los Angeles, CA.

WHAT YOU CAN DO

We don't know if the hacker successfully retrieved any data, but we strenuously recommend that if you used AuthorizeNet as your payment gateway on our site between May 1st and May 16th, you keep a close eye on your credit card transactions and report to your issuing bank that your card may have been compromised. Equifax also provides Identity Theft Prevention Tips, which provides additional steps that you can take, including instructions for obtaining a free copy of your credit report and how to place a fraud alert and/or credit freeze on your report.

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
888-766-0008

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
888-397-3742

TransUnion
PO Box 2000
Chester, PA 19016
www.transunion.com
800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You may also contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

State Attorneys General: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report.

The State of California has a web site with further information to help consumers when their data has been breached: https://oag.ca.gov/privacy/other-privacy/breach-help-tips-for-consumers

FOR MORE INFORMATION
We are deeply committed to our customers, and I am profoundly upset that this breach occurred. We will continue to do everything in our power to ensure that this does not happen again in the future, and I hope that you can accept my heartfelt apology. If you have any questions, please do not hesitate to contact us at answers@blackphoenixalchemylab.com.

With all my heart, I am so, so sorry.

Elizabeth Barrial
President
Black Phoenix, Inc.