855-774-5263
5637 Carolina Beach Rd #15015
Wilmington, NC 28412

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

August 20, 2026

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to provide you with information regarding an incident that may have exposed sensitive information transmitted between you and Primary Jane, LLC (the "Company").

We assure you that the confidentiality and security of our clients' information is of upmost importance to us, and we want you to know that we take seriously the responsibility to protect that information. We sincerely regret that this incident occurred, and we apologize for any inconvenience it may have caused you. Please review the rest of this letter for details about the incident and our response.

What Happened

On July 21, 2026, the Company's malware protection software detected an anomaly on the Company's website. A subsequent investigation, with assistance from our outside information technology ("IT") support team, determined that an unauthorized third-party surreptitiously installed malicious code on our website that allowed them to harvest digital credit card information as transactions were processed. This code was active from July 13, 2026, to July 21, 2026, before being detected and removed.

What Information Was Involved

As part of our investigation, we were able to determine which customers made purchases during the time the code was active. It was determined that you were one of the affected customers.

At this time, we do not have any knowledge that your credit card or personal information used to make a purchase on the Company's website has been misused. Out of an abundance of caution, however, we are notifying persons whose information was exposed so that you can take steps to protect your information, if you feel it is appropriate to do so.

The information exposed includes credit/debit card numbers, expiration dates, CVV codes, and the name and zip code associated with the card.

What We Are Doing

The Company has taken steps to address the threat, including by notifying and working with the Company's outside IT support to secure the Company's website. In addition to working with IT support, we have engaged professionals experienced in handling these types of incidents to assist us with our response and to assess the full scope of information impacted. We have also notified and are cooperating with law enforcement and state regulators in connection with this incident.

The Company is committed to maintaining the privacy and confidentiality of the information we gather from clients, and we have taken precautions to safeguard it. Moving forward we will work with cybersecurity professionals to evaluate and modify our practices and internal controls to adapt to evolving criminal threats. Certain additional security measures have already been implemented. For example, you may have noticed that we recently required a password reset for account holders and are now offering multi-factor authentication related to account logins. Other measures have been taken that are not directly visible to customers.

What You Can Do

You should review your credit/debit card records to see if the card was used on the Company's website between July 13 and July 21. It is advisable that you cancel any credit/debit card used to purchase products from Primary Jane during that window.

Additionally, the enclosed "Further Information" document provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. You should always remain vigilant in reviewing your financial account statements and credit reports for suspicious activity and to detect errors.

For More Information

If you have questions that are not answered by this letter or the enclosed information, you may contact us between 9 AM and 4:30 PM ET, Monday – Friday, excluding holidays. Please feel free to contact us as you normally would with those questions at 855-774-5263.

Sincerely,

Primary Jane, LLC

_____

Jeff McGurren, President

(Enclosure)

FURTHER INFORMATION TO HELP PROTECT YOUR PRIVACY

Place a fraud alert on your credit report. You have the option of placing a fraud alert on your credit report. A fraud alert is free of charge and easy to place. You may contact toll-free any one of the three major credit bureaus listed below. As soon as one bureau confirms your report, the others are simultaneously notified on your behalf.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

Obtain a copy of your free credit report. You may also obtain a free copy of your credit report from each of the three major credit reporting bureaus once every 12 months by visiting 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, Georgia 30348. It is recommended that you monitor your free credit reports for incidents of fraud and identity theft. You may purchase a copy of your credit report by contacting one of the three major credit reporting bureaus above.

Place a 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.

Review your account statements and monitor credit reports. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your financial account statements and monitoring your free credit reports for unauthorized access. Doing so can help you spot problems and address them quickly.

Notify law enforcement of any suspicious activity. You should also notify the appropriate law enforcement authorities, your state attorney general, and/or the U.S. Federal Trade Commission (FTC) of any suspected identity theft.

Federal and State resources to protect against identity theft. You can find additional information to help protect yourself from identity theft, including information about fraud alerts and credit report security freezes, by contacting one of the three major credit bureaus listed above, or by visiting the FTC's website at www.ftc.gov/idtheft, by calling 1-877-ID-THEFT (1-877-438-4338), or by writing to the Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580. You may also wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling (877) 566-7226, or by writing to the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699.