Patterson-Schwartz Real Estate
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

[redacted]

November 6, 2025

NOTICE OF DATA BREACH

Dear [redacted]

We are writing to let you know about a data security incident that may have involved some of your personal information. Patterson-Schwartz & Associates, Inc., dba Patterson-Schwartz Real Estate values your privacy and deeply regrets that this incident occurred. We are taking this matter very seriously and are providing you with details of what happened, what we are doing, and how you can protect yourself.

WHAT HAPPENED?

On or about May 14 and May 29, 2025, unauthorized third parties gained access to two internal email accounts. These breaches were the result of sophisticated phishing attacks and were not breaches of our core systems. As soon as we detected the activity, we immediately secured the compromised email accounts and launched a thorough investigation with the assistance of a cybersecurity firm.

WHAT INFORMATION WAS INVOLVED?

Based on our investigation, the unauthorized actors may have viewed or accessed the contents of the compromised email accounts. The specific types of information present in the emails and attachments varied, but may have included:

- Names
- Email addresses
- Phone numbers
- Mailing addresses
- Birth dates
- Bank account and credit card numbers
- Driver's license numbers
- Social Security numbers

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

WHAT WE ARE DOING

We immediately took action to secure the affected email accounts and have implemented enhanced security controls across our email platform to prevent a recurrence. Our investigation is ongoing, and we are working with external cybersecurity experts to determine the full scope of the incident. We are reinforcing our internal security measures, including enhanced multi-factor authentication (MFA) for all sales associates and employees and conducting additional cybersecurity training to help our email users recognize and avoid future phishing attempts to prevent a recurrence of such attacks and to protect the privacy of our valued customers.

WHAT YOU CAN DO

We encourage you to take the following steps to protect yourself:

- Please be extremely cautious of any suspicious emails, particularly those that appear to be from our company or its representatives. We will not call, email, or text you requesting your password or personal information.
- Closely monitor your financial and online accounts for any suspicious activity and report unauthorized activity to the relevant institution immediately.
- In response to the incident, we are providing you with 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 months from the date of enrollment when changes occur to your 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.
- Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on how you can enroll and other steps you can take to protect your information.

FOR MORE INFORMATION

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at **1-833-594-0868** and supply the fraud specialist with the following unique code to receive [redacted] We value your trust and are committed to protecting your information.

Sincerely,

Donna Greenspan, Chief Executive Officer &
Jason Giles, President
7234 Lancaster Pike
Suite 200B
Hockessin, DE 19707
302-234-5270
toll-free 877-456-4663

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

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you 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 access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies to request a copy of your credit report or for general inquiries is provided below:

	Equifax	**Experian**	**TransUnion**
Contact Information	(866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	(800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

We recommend 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.

- **Credit Report Monitoring**

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **51082FF333C4**. 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. 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.

- **Take Advantage of Additional Free Resources on Identity Theft**

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400.

North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000

OTHER IMPORTANT INFORMATION

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.