



<<Date>> (Format: Month Day, Year)

<<FIRST\_NAME>> <<MIDDLE\_NAME>> <<LAST\_NAME>> <<SUFFIX>>  
<<ADDRESS\_1>>  
<<ADDRESS\_2>>  
<<CITY>>, <<STATE\_PROVINCE>> <<POSTAL\_CODE>>  
<<COUNTRY>>

<< b2b\_text\_1 (Subject: Notice of Data Breach / Subject: Notice of Security Incident)>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

We are writing to inform you of a recent data security incident experienced by Glazier, Glazier & Dietrich PA (“GGD”) that may have affected your personally identifiable information. GGD takes the privacy and security of all information within its possession very seriously. We want to emphasize that GGD has no evidence of the misuse or attempted misuse of your personally identifiable information.

### **What Happened?**

On February 17, 2025, GGD identified suspicious activity on its network. In response, GGD took immediate steps to secure its digital environment and promptly launched an investigation. In so doing, GGD engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On April 29, 2025, GGD learned that your personally identifiable information may have been impacted in connection with the incident, which is the reason for this notification. GGD then worked diligently to identify information required to effectuate your notification. **Notably, based on the investigation, GGD has no evidence of the misuse or attempted misuse of any of your potentially impacted information.**

### **What Information Was Involved?**

The information potentially impacted in connection with this incident included your <<b2b\_text\_2 (“Impacted Data name and data elements ”)>>.

### **What Are We Doing?**

As soon as GGD discovered this incident, GGD took the steps described above. In addition, GGD implemented measures to enhance security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future.

Although GGD has no evidence of the misuse or attempted misuse of any potentially impacted information, is providing you with information about steps that you can take to help protect your information and is offering <<ServiceTerminMonths>> months of complimentary identity monitoring services through Kroll - a data breach and recovery services expert. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number (S\_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](https://info.krollmonitoring.com). Additional information describing your services is included with this letter.

**What You Can Do:**

Please review the enclosed Recommended Steps section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

To reiterate, at this time there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering as a precaution. Kroll representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

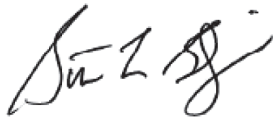
**For More Information:**

You will find detailed instructions for activating monitoring on the enclosed Recommended Steps document.

If you have questions, please call (866) 461-2568, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Please know that GGD takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott L. Glazier". The signature is fluid and cursive, with the first name "Scott" being the most prominent part.

Scott L. Glazier, Esq.  
President  
Glazier, Glazier & Dietrich PA



## Recommended Steps to help Protect your Information

### TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

#### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data (for instance, when a new line of credit is applied for in your name). If you do not recognize the activity, you will have the option to call a Kroll fraud specialist who will be able to help you determine if it is an indicator of identity theft.

#### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

#### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

#### Contact information for the three nationwide credit reporting agencies:

**Equifax**, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alerts.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security Freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html). You have the right to obtain a police report if you are a victim of identity theft.