



Secure Processing Center  
25 Route 111, P.O. Box 1048  
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<City>>, <<State>> <<Zip>>  
<<Country>>  
\*\*\*Postal IMB Barcode

March 6, 2026

<<VARIABLE DATA 1>>

Dear <<Full Name>>:

We are writing to provide you with information regarding a data security incident (the “Incident”) experienced by Cardone Law Firm (“Cardone Law” or “we”) that may have involved your personal information. This letter provides you with more information about this Incident, our response, and guidance on where to direct your questions. As a precaution, we have also provided steps you can take to protect your information, including the ability to enroll in credit monitoring services that we are offering free of charge for twenty-four (24) months.

**What Happened?**

On August 25, 2025, we discovered some suspicious activity within our computer systems. Upon discovery, we immediately began an investigation and took steps to contain the situation, including proactively taking systems offline, changing passwords, deploying advanced security and detection software, engaging leading cybersecurity professionals to assist, and restoring systems in a safe environment.

Through our investigation, we identified that files containing your Information were obtained by an unauthorized party. Our investigation did not identify any evidence of misuse of your information for fraud or identity theft related to the Incident.

**What Information Was Involved?**

Our investigation determined that the following types of information were impacted as a result of this Incident: Name, <<Breached Elements>>. As mentioned, there is no evidence that your information was misused for fraud or identity theft as a result of this Incident.

**What We Are Doing.**

We take the security of client information in our care seriously. Upon identifying this Incident, we immediately implemented additional measures to further improve the security of our systems and practices, worked with leading cybersecurity and privacy firms to aid in our investigation and response, and after determining unauthorized activity occurred on our systems, began analyzing the information involved to confirm the identities of potentially affected individuals to notify them.

**What Can You Do?**

To help protect your identity, we are offering complimentary access to Epiq – Privacy Solutions ID for twenty-four (24) months. To start monitoring your personal information, please follow the steps below.

- 1) Visit [www.privacysolutionsid.com](http://www.privacysolutionsid.com) and click “Activate Account”.
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form.

- 3) Complete the identity verification process.
- 4) You will receive a separate email from [noreply@privacysolutions.com](mailto:noreply@privacysolutions.com) confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page.
- 5) Enter your log-in credentials.
- 6) You will be directed to your dashboard and activation is complete.

The deadline to enroll is May 31, 2026. If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at 866-675-2006, Monday - Friday 9:00 a.m. – 5:30 p.m. Eastern Standard Time.

Although we are unaware of any fraud or identity theft in connection with this Incident, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

**For More Information.**

If you have any questions, please call us at 844-558-4349 Monday - Friday between 9:00 a.m. – 9:00 p.m. Eastern Time (excluding some U.S. national holidays).

Sincerely,



Clifford E. Cardone  
Founder

Encl.

## ADDITIONAL RESOURCES

### Contact information for the three (3) nationwide credit reporting agencies:

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

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

**TransUnion**, PO Box 2000, Chester, PA 19016, <https://www.transunion.com/data-breach-help>, 1-833-799-5355

**Free Credit Report.** It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) 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 Massachusetts residents:** You may obtain one (1) 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 Alert.** You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

**Security Freeze.** You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) 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 them 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 five years; and (5) any applicable incident report or complaint with a law enforcement agency or Department 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.

**FTC 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 FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid 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).

**Reporting of identity theft and obtaining a police report.** You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

**For California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

**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.

**For Pennsylvania Residents:** You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15<sup>th</sup> Floor, Strawberry Square, Harrisburg, PA 17120, [www.attorneygeneral.gov](http://www.attorneygeneral.gov), 1-800-441-2555.