Frequently Asked Questions

Is this letter real?
Yes, the letter is real.

What information of mine was on the server? I have never had an interaction with the Springfield Police Department.

While the information was on the police server, that does not mean it was necessarily related to a criminal incident. Rather, the information could have been obtained during a number of routine, noncriminal activities such:

- Telephone call to the Police Department
- Driver of a motor vehicle issued a summons
- Owner of a motor vehicle issued a summons
- Driver and all passengers of a motor vehicle accident
- Owner of a vehicle involved in a motor vehicle accident
- Reporting party of an incident
- Reporting party of a lost/missing report
- Subject listed on a Field Interview Card
- Witness to an incident (motor vehicle accident, etc)
- Caller for overnight parking
- Fire arms registered to the home
- Court order for resident

Why did the Township have my personal information? I am not currently / have never before been a resident.
Our records indicate you were either named in or were previously engaged with the Springfield Police Department, either as a party in a police report narrative or in some other indirect encounter. The Township remains vigilant in its efforts to protect confidential information of its citizens and visitors, and we have implemented additional safeguards to help prevent additional cyber-attacks.

I received a letter addressed to my deceased family member. Is this real? Why would my family member have ever been in contact with the Springfield Police Department?

Yes, the letter is real.

Why did I receive a letter addressed to the parent/guardian of John Q. Minor? Is my information impacted, too, or just my child / dependent's?

Only the child/dependent's listed information is potentially impacted. The letter was addressed "To the Parent/Guardian of [name]" because the child is believed to be under 18 years of age.

What happened?

During a network security review, we identified suspicious activity on our Police Department management server. Once we discovered this suspicious activity, we immediately initiated an internal investigation and IT remediation. We also engaged external forensic IT experts to assist in our investigation, and the incident was

subject to ongoing police investigation. The forensic IT experts have confirmed that there was unauthorized access to the server between Feb. 22, 2017 and March 9, 2017, when the threat was eliminated.

What information may be impacted?

The information may have included your full name, SSN, driver's license or state card identification number, State and Federal Bureau Investigation number, credit card numbers provided to authorities or was subject to police investigation, birth date, address, telephone number and police narrative. However, not everyone was potentially impacted in the same way, and you can contact our call center to learn what information of yours may have been potentially exposed.

Was my information disclosed?

We have no indication that any personal information has been accessed or used inappropriately. We have sent you this letter as a precaution because some of your information is believed to have been on the server.

Did you report the incident to law enforcement?

Yes. We continue to work closely with the FBI, and we have notified the New Jersey State Police, all applicable state agencies, and all three credit bureaus. We will pursue prosecution of these criminals to the full extent of U.S. law.

Is this server still being used by Police Department?

No.

Was any other Township system affected?

No. This incident was isolated to one server and does not impact any other systems at the Township. The threat to the impacted server was eliminated on March 9, 2017.

What is the Township doing to ensure that this does not happen again?

The Township remains vigilant in its efforts to protect confidential information of its citizens and visitors and has already implemented additional safeguards to help prevent additional cyber-attacks. We also continue to work closely with the FBI, and we have notified the New Jersey State Police, all applicable state agencies, and all three credit bureaus. Lastly, we will pursue prosecution of these criminals to the full extent of U.S. law.

Do you suspect that my information has been used fraudulently? Has anyone been adversely affected as a result of this incident?

We have no indication that any personal information has been viewed or used inappropriately at this time. However, out of an abundance of caution, we are providing notice to individuals identified as potentially affected.

How do I obtain a free copy of my credit report?

Consumers may also 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 print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Is there anything I should do to protect myself?

The Federal Trade Commission provides free tips on how to avoid identity theft. You can access those tips by visiting www.ftc.gov/idtheft.

Further, below please find general information on identity theft protection.

You may also obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com.

What recourse do I have for my deceased family member? Can I use the credit monitoring services mentioned in the letter?

Credit monitoring services are not available for deceased individuals. However, there are steps you can take to request a copy of his/her credit report. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual's credit report. An executor or surviving spouse can also request that the following two notices be placed on a deceased individual's credit report:

- "Deceased – Do not issue credit"; or
- "If an application is made for credit, please notify the following person(s) (e.g. surviving relative, executor/trustee of the estate and/or local law enforcement agency – notifying the relationship)."

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

General Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by 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 one or more of the three national credit reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is

not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority 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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may contact the Attorney General's Office at http://www.riag.ri.gov/ or (401)
274-4400.

Fraud Alerts: There are also two types of fraud alerts that 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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit

grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.