

15708



State of New York
County of Broome Government Offices

Broome County Department of Personnel

Jason T. Garnar, County Executive · Thomas H. Behan, Personnel Officer

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Broome County Government ("County") is writing to notify you of an incident that may affect the security of some of your personal information. We take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On January 2, 2019 the County became aware of changes to a County employee's direct deposit information. The County's internal IT team immediately launched an investigation into the nature and scope of the incident. On or around January 7, 2019, the County's investigation identified unauthorized access to numerous County employee email accounts and County employee PeopleSoft accounts as a result of a credentials harvesting phishing email. We immediately launched an investigation to determine what may have happened and what information may have been affected. Working together with a leading computer forensics expert, our investigation determined that an unauthorized individual or individuals accessed the email account between November 20, 2018 and January 2, 2019.

Because we were unable to determine which email messages in the accounts may have been opened or taken by the unauthorized actor, we reviewed the contents of the email accounts to identify what personal information was stored within it. On April 1, 2019, after a thorough review of the email accounts, we confirmed that the affected email accounts contained sensitive information, and identified the individuals potentially impacted by this incident. Once we confirmed the individuals who were potentially impacted, the County worked to identify the best possible contact information for the impacted individuals and then began preparing an accurate written notice of this incident.

What Information Was Affected? The following County divisions/departments were impacted by this incident:

- Willow Point Nursing Home and Rehabilitation & Nursing Center
- Greater Binghamton Airport
- Broome County Department of Social Services
- Broome County District Attorney's Office
- Broome County Office for Aging
- Broome County Office of Employment and Training
- Broome County Office of Emergency Services
- Broome County Department of Health
- Broome County Department of Planning and Economic Development
- Broome County Department of Probation
- Broome County Department of Public Transportation
- Broome County Department of Public Works - Highway Division
- Broome County Veterans Services Agency

The County believes that the unauthorized actor may have had access to information related to certain individuals who received care from or are associated with the above referenced list of County departments/offices.

With the exception of direct deposit information for certain County employees, the County cannot confirm whether any specific information within the affected email accounts was actually accessed, viewed, or acquired without permission. They are providing this notification out of an abundance of caution to anyone whose information was accessible within the email accounts. The following types of your information were located in an email or attachment and may have been accessed or acquired by an unauthorized user: <<ClientDef1(Breach Details Variable Text)>><<ClientDef2(Breach Details Variable Text)>>.

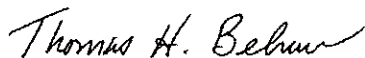
What Are We Doing? Information privacy and security are among our highest priorities. The County has strict security measures to protect the information in our possession. Upon learning of this incident, we immediately reset passwords for the impacted employees and subsequently reset all County employee passwords. We are currently implementing additional technical safeguards including multi-factor authentication, as well as training and education for employees to prevent similar future incidents.

What Can You Do? Although we are not aware of any actual or attempted misuse of your information, we arranged to have Kroll monitor your identity for 18 months at no cost to you as an added precaution. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to activate and receive these services. The County will cover the cost of this service; however, you will need to activate the identity monitoring service yourself.

For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-775-4209 (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m., ET.

We sincerely regret any inconvenience this incident may cause you. The County remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,



Thomas H. Behan
Personnel Officer

Steps You Can Take to Protect Your Information

Activate Identity Monitoring.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for eighteen (18) months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until **September 26, 2019** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

We recommend that you regularly review any Explanation of Benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.