



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

The City of Bedford is writing to inform you of a recent data security incident that involved some of your personal information. We understand that news like this can be concerning, and we sincerely regret this situation occurred. Protecting the personal information entrusted to us is a responsibility we take very seriously, and we want to provide you with information about what happened, what we are doing in response, and steps you can take to help protect yourself.

What Happened?

On April 9, 2025, we detected suspicious activity within a portion of the City's computer network. We immediately took steps to secure our systems and began working with independent cybersecurity experts to investigate the activity and determine what occurred.

Through that investigation, we learned that an unauthorized third party accessed a limited portion of our network between April 5 and April 9, 2025. After identifying the files that may have been impacted, we engaged a specialized data-review firm to analyze those files and determine what information they contained. We received the results of that review in March 2026 and have since worked to confirm contact information so we could notify individuals whose information may have been affected.

What Information Was Involved?

The information involved may have included some of your personal information, which includes your: <<Breached Elements>>.

What We Are Doing.

Upon discovering this incident, we promptly took steps to secure our network and launched a thorough investigation with the assistance of independent cybersecurity professionals. We also notified law enforcement of the incident, which did not delay this notice.

In addition, we have taken steps to further strengthen the security of our systems and reduce the risk of a similar event occurring in the future.

What You Can Do.

We encourage you to remain vigilant for signs of fraud or unauthorized activity by reviewing your financial account statements and monitoring your credit reports. Additional information about steps you can take to help protect your personal information is included on the next page of this letter.

While we are not aware of any misuse of your personal information related to this incident at this time, we are offering you a complimentary <<12/24>>-month membership to Epiq - Privacy Solutions ID to help provide an added layer of protection.

To enroll, please:

- 1) Visit www.privacysolutionsid.com by <<Enrollment Deadline>> and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process

After you complete the verification process, your account is active and you will receive an email from noreply@privacysolutions.com confirming that your account was set up. That email will contain an “Access Your Account” link that you can use to access your account. If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions, please call (866) 675-2006 any time Monday through Friday from 9:00 a.m. to 5:30 p.m. Eastern Time.

For More Information.

If you have questions or need additional assistance, please contact us at (888)504-8543, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central time, and a representative will be happy to help. We regret any concern or inconvenience this situation may cause. The City remains committed to protecting the information entrusted to us and to keeping our community informed.

Sincerely,

City of Bedford
City Manager’s Office

ADDITIONAL STEPS YOU CAN TAKE

Remain Vigilant

We encourage you to remain vigilant for signs of fraud or identity theft by regularly reviewing your account statements and monitoring your credit reports. If you see transactions or activity that you do not recognize, contact your financial institution immediately.

You may obtain a free copy of your credit report once every week from each of the three major consumer reporting agencies by visiting www.annualcreditreport.com or calling (877) 322-8228.

If you identify errors on your credit report, please contact the appropriate consumer reporting agency:

Equifax

PO Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

PO Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

You may also find additional information about protecting yourself from identity theft at www.IdentityTheft.gov or by contacting the Federal Trade Commission:

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(877) 438-4338
www.ftc.gov

Consider Placing a Fraud Alert or Security Freeze

Consumer reporting agencies offer security freezes and fraud alerts, which are tools that may help protect your credit. You can also contact the Federal Trade Commission for more details on a fraud alert or security freeze.

Fraud Alert

A fraud alert places a notice on your credit file advising potential creditors to take additional steps to verify your identity before issuing credit. Fraud alerts last for one year but may be renewed. You can contact any of the consumer reporting agencies to place a fraud alert.

Security Freeze

A security freeze restricts access to your credit report, making it more difficult for someone to open a new account in your name. You must contact each consumer reporting agency individually to request a security freeze, and they may require you provide them your name, Social Security number, birthdate, and contact information. There is no charge for placing a security freeze.

Report Suspicious Activity

If you believe you are the victim of fraud or identity theft, you may contact the Federal Trade Commission or your state attorney general. You also have the right to file a police report regarding suspected identity theft.

Fair Credit Reporting Act

You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, dispute inaccurate or incomplete information, and request that consumer reporting agencies correct or remove information that cannot be verified. Additional information about your rights under the FCRA is available at:

www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

Additional State Resources

Your state attorney general may provide additional information about fraud alerts, security freezes, and protecting yourself from identity theft.

Maryland Residents

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.com

New York Residents

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

North Carolina Residents

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdog.gov

Washington, DC Residents

Office of the Attorney General
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

Rhode Island Residents

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

This event impacted <<#>> Rhode Island residents.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

The City of Bedford is writing to inform you of a recent data security incident that involved some of your personal information. We understand that news like this can be concerning, and we sincerely regret this situation occurred. Protecting the personal information entrusted to us is a responsibility we take very seriously, and we want to provide you with information about what happened, what we are doing in response, and steps you can take to help protect yourself.

What Happened?

On April 9, 2025, we detected suspicious activity within a portion of the City's computer network. We immediately took steps to secure our systems and began working with independent cybersecurity experts to investigate the activity and determine what occurred.

Through that investigation, we learned that an unauthorized third party accessed a limited portion of our network between April 5 and April 9, 2025. After identifying the files that may have been impacted, we engaged a specialized data-review firm to analyze those files and determine what information they contained. We received the results of that review in March 2026 and have since worked to confirm contact information so we could notify individuals whose information may have been affected.

What Information Was Involved?

The information involved may have included some of your personal information, which includes your: <<Breached Elements>>.

What We Are Doing.

Upon discovering this incident, we promptly took steps to secure our network and launched a thorough investigation with the assistance of independent cybersecurity professionals. We also notified law enforcement of the incident, which did not delay this notice.

In addition, we have taken steps to further strengthen the security of our systems and reduce the risk of a similar event occurring in the future.

What You Can Do.

We encourage you to remain vigilant for signs of fraud or unauthorized activity by reviewing your financial account statements and monitoring your credit reports. Additional information about steps you can take to help protect your personal information is included on the next page of this letter.

For More Information.

If you have questions or need additional assistance, please contact us at (888)504-8543, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central time, and a representative will be happy to help. We regret any concern or inconvenience this situation may cause. The City remains committed to protecting the information entrusted to us and to keeping our community informed.

Sincerely,

City of Bedford
City Manager's Office

ADDITIONAL STEPS YOU CAN TAKE

Remain Vigilant

We encourage you to remain vigilant for signs of fraud or identity theft by regularly reviewing your account statements and monitoring your credit reports. If you see transactions or activity that you do not recognize, contact your financial institution immediately.

You may obtain a free copy of your credit report once every week from each of the three major consumer reporting agencies by visiting www.annualcreditreport.com or calling (877) 322-8228.

If you identify errors on your credit report, please contact the appropriate consumer reporting agency:

Equifax

PO Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

PO Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

You may also find additional information about protecting yourself from identity theft at www.IdentityTheft.gov or by contacting the Federal Trade Commission:

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(877) 438-4338
www.ftc.gov

Consider Placing a Fraud Alert or Security Freeze

Consumer reporting agencies offer security freezes and fraud alerts, which are tools that may help protect your credit. You can also contact the Federal Trade Commission for more details on a fraud alert or security freeze.

Fraud Alert

A fraud alert places a notice on your credit file advising potential creditors to take additional steps to verify your identity before issuing credit. Fraud alerts last for one year but may be renewed. You can contact any of the consumer reporting agencies to place a fraud alert.

Security Freeze

A security freeze restricts access to your credit report, making it more difficult for someone to open a new account in your name. You must contact each consumer reporting agency individually to request a security freeze, and they may require you provide them your name, Social Security number, birthdate, and contact information. There is no charge for placing a security freeze.

Report Suspicious Activity

If you believe you are the victim of fraud or identity theft, you may contact the Federal Trade Commission or your state attorney general. You also have the right to file a police report regarding suspected identity theft.

Fair Credit Reporting Act

You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, dispute inaccurate or incomplete information, and request that consumer reporting agencies correct or remove information that cannot be verified. Additional information about your rights under the FCRA is available at:

www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

Additional State Resources

Your state attorney general may provide additional information about fraud alerts, security freezes, and protecting yourself from identity theft.

Maryland Residents

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.com

New York Residents

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

North Carolina Residents

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdog.gov

Washington, DC Residents

Office of the Attorney General
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

Rhode Island Residents

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

This event impacted <<#>> Rhode Island residents.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
To the Parent or Guardian of:
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<Date>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <<Full Name>>,

The City of Bedford is writing to inform you of a recent data security incident that involved some of your child's personal information. We understand that news like this can be concerning, and we sincerely regret this situation occurred. Protecting the personal information entrusted to us is a responsibility we take very seriously, and we want to provide you with information about what happened, what we are doing in response, and steps you can take to help protect your child.

What Happened?

On April 9, 2025, we detected suspicious activity within a portion of the City's computer network. We immediately took steps to secure our systems and began working with independent cybersecurity experts to investigate the activity and determine what occurred.

Through that investigation, we learned that an unauthorized third party accessed a limited portion of our network between April 5 and April 9, 2025. After identifying the files that may have been impacted, we engaged a specialized data-review firm to analyze those files and determine what information they contained. We received the results of that review in March 2026 and have since worked to confirm contact information so we could notify individuals whose information may have been affected.

What Information Was Involved?

The information involved may have included some of your child's personal information, which includes their: <<breached elements>>.

What We Are Doing.

Upon discovering this incident, we promptly took steps to secure our network and launched a thorough investigation with the assistance of independent cybersecurity professionals. We also notified law enforcement of the incident, which did not delay this notice.

In addition, we have taken steps to further strengthen the security of our systems and reduce the risk of a similar event occurring in the future.

What You Can Do.

We encourage you to remain vigilant for signs of fraud or unauthorized activity by reviewing your child's financial account statements and monitoring their credit reports. Additional information about steps you can take to help protect your child's personal information is included on the next page of this letter.

For More Information.

If you have questions or need additional assistance, please contact us at (888) 504-8543, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central time, and a representative will be happy to help. We regret any concern or inconvenience this situation may cause. The City remains committed to protecting the information entrusted to us and to keeping our community informed.

Sincerely,

City of Bedford
City Manager's Office

ADDITIONAL STEPS YOU CAN TAKE

Remain Vigilant

We encourage you to remain vigilant for signs of fraud or identity theft by regularly reviewing your child's account statements and monitoring their credit reports. If you see transactions or activity that you do not recognize, contact your child's financial institution immediately.

You may obtain a free copy of your child's credit report once every week from each of the three major consumer reporting agencies by visiting www.annualcreditreport.com or calling (877) 322-8228.

If you identify errors on your child's credit report, please contact the appropriate consumer reporting agency:

Equifax

PO Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

PO Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

You may also find additional information about protecting your child from identity theft at www.IdentityTheft.gov or by contacting the Federal Trade Commission:

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(877) 438-4338
www.ftc.gov

Consider Placing a Fraud Alert or Security Freeze

Consumer reporting agencies offer security freezes and fraud alerts, which are tools that may help protect your child's credit. You can also contact the Federal Trade Commission for more details on a fraud alert or security freeze.

Fraud Alert

A fraud alert places a notice on your child's credit file advising potential creditors to take additional steps to verify your child's identity before issuing credit. Fraud alerts last for one year but may be renewed. You can contact any of the consumer reporting agencies to place a fraud alert.

Security Freeze

A security freeze restricts access to your child's credit report, making it more difficult for someone to open a new account in their name. You must contact each consumer reporting agency individually to request a security freeze, and they may require you provide them your child's name, Social Security number, birthdate, and contact information. There is no charge for placing a security freeze.

Report Suspicious Activity

If you believe your child is the victim of fraud or identity theft, you may contact the Federal Trade Commission or your state attorney general. You also have the right to file a police report regarding suspected identity theft.

Fair Credit Reporting Act

Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, dispute inaccurate or incomplete information, and request that consumer reporting agencies correct or remove information that cannot be verified. Additional information about your child's rights under the FCRA is available at:

www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

Additional State Resources

Your state attorney general may provide additional information about fraud alerts, security freezes, and protecting your child from identity theft.

Maryland Residents

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.com

New York Residents

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

North Carolina Residents

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdog.gov

Washington, DC Residents

Office of the Attorney General
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

Rhode Island Residents

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

This event impacted <<#>> Rhode Island residents.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
To the Parent or Guardian of:

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

<Date>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <<Full Name>>,

The City of Bedford is writing to inform you of a recent data security incident that involved some of your child's personal information. We understand that news like this can be concerning, and we sincerely regret this situation occurred. Protecting the personal information entrusted to us is a responsibility we take very seriously, and we want to provide you with information about what happened, what we are doing in response, and steps you can take to help protect your child.

What Happened?

On April 9, 2025, we detected suspicious activity within a portion of the City's computer network. We immediately took steps to secure our systems and began working with independent cybersecurity experts to investigate the activity and determine what occurred.

Through that investigation, we learned that an unauthorized third party accessed a limited portion of our network between April 5 and April 9, 2025. After identifying the files that may have been impacted, we engaged a specialized data-review firm to analyze those files and determine what information they contained. We received the results of that review in March 2026 and have since worked to confirm contact information so we could notify individuals whose information may have been affected.

What Information Was Involved?

The information involved may have included some of your child's personal information, which includes their: <<Breached Elements>>.

What We Are Doing.

Upon discovering this incident, we promptly took steps to secure our network and launched a thorough investigation with the assistance of independent cybersecurity professionals. We also notified law enforcement of the incident, which did not delay this notice.

In addition, we have taken steps to further strengthen the security of our systems and reduce the risk of a similar event occurring in the future.

What You Can Do.

We encourage you to remain vigilant for signs of fraud or unauthorized activity by reviewing your child's financial account statements and monitoring their credit reports. Additional information about steps you can take to help protect your child's personal information is included on the next page of this letter.

While we are not aware of any misuse of your child's personal information related to this incident at this time, we are offering your child a complimentary <<12/24>>-month membership to Epiq Privacy Solutions ID Minor Monitoring services to help provide an added layer of protection.

To activate those services, you must establish an Epiq Privacy Solutions ID account on behalf of your child. You will be asked to create an account, verify your identity, and then select up to ten details (such as their medical ID or Social Security number) concerning your child that you want monitored. More detailed instructions on the enrollment process are below.

To enroll please:

1. Visit privacysolutions.com by <<Enrollment Deadline>> and click "Activate Account"
2. Enter the following activation code <<Activation Code>> and complete the enrollment form
3. Complete the identity verification process
4. Access the login page using the "Access Your Account" link in the email from noreply@privacysolutions.com
5. Enter your login credentials
6. Select "Monitored Information" on the dashboard
7. Add the information for your child that you want monitored

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID Minor Monitor, please call (866) 675-2006 any time Monday through Friday, 9:00 a.m. to 5:30 p.m. Eastern Time.

For More Information.

If you have questions or need additional assistance, please contact us at (888)504-8543, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central time, and a representative will be happy to help. We regret any concern or inconvenience this situation may cause. The City remains committed to protecting the information entrusted to us and to keeping our community informed.

Sincerely,

City of Bedford
City Manager's Office

ADDITIONAL STEPS YOU CAN TAKE

Remain Vigilant

We encourage you to remain vigilant for signs of fraud or identity theft by regularly reviewing your child's account statements and monitoring their credit reports. If you see transactions or activity that you do not recognize, contact your child's financial institution immediately.

You may obtain a free copy of your child's credit report once every week from each of the three major consumer reporting agencies by visiting www.annualcreditreport.com or calling (877) 322-8228.

If you identify errors on your child's credit report, please contact the appropriate consumer reporting agency:

Equifax

PO Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

PO Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

You may also find additional information about protecting your child from identity theft at www.IdentityTheft.gov or by contacting the Federal Trade Commission:

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(877) 438-4338
www.ftc.gov

Consider Placing a Fraud Alert or Security Freeze

Consumer reporting agencies offer security freezes and fraud alerts, which are tools that may help protect your child's credit. You can also contact the Federal Trade Commission for more details on a fraud alert or security freeze.

Fraud Alert

A fraud alert places a notice on your child's credit file advising potential creditors to take additional steps to verify your child's identity before issuing credit. Fraud alerts last for one year but may be renewed. You can contact any of the consumer reporting agencies to place a fraud alert.

Security Freeze

A security freeze restricts access to your child's credit report, making it more difficult for someone to open a new account in their name. You must contact each consumer reporting agency individually to request a security freeze, and they may require you provide them your child's name, Social Security number, birthdate, and contact information. There is no charge for placing a security freeze.

Report Suspicious Activity

If you believe your child is the victim of fraud or identity theft, you may contact the Federal Trade Commission or your state attorney general. You also have the right to file a police report regarding suspected identity theft.

Fair Credit Reporting Act

Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, dispute inaccurate or incomplete information, and request that consumer reporting agencies correct or remove information that cannot be verified. Additional information about your child's rights under the FCRA is available at:

www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

Additional State Resources

Your state attorney general may provide additional information about fraud alerts, security freezes, and protecting your child from identity theft.

Maryland Residents

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.com

New York Residents

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

North Carolina Residents

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdog.gov

Washington, DC Residents

Office of the Attorney General
400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

Rhode Island Residents

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

This event impacted << #>> Rhode Island residents.