# City of Whitehall Data Breach FAQ

**(1) What happened?**

On May 27, 2022, City of Whitehall detected that a ransomware infection began encrypting files stored on our network. Upon learning of this issue, we contained the threat by disabling and isolating the affected systems, and immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handing these types of incidents. The investigation determined that certain impacted files containing personal information may have been removed from our network by the perpetrator.

**(2) How did this happen?**

On May 27, 2022, City of Whitehall became aware that an unauthorized party may have obtained access to the network. Upon learning of this issue, we commenced a prompt and thorough investigation with external cybersecurity professionals. The investigation determined the unauthorized party exploited a software defect to gain access into the network.

**(3) Why did I receive a notification from City of Whitehall?**

After learning of the issue, the City of Whitehall moved to determine what information may have been contained in the network. The investigation determined that certain impacted files containing your personal information may have been removed from our network by the perpetrator.

To date we have no evidence that any of the information contained in the network was specifically misused. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident.

**(4) I received a notification from City of Whitehall about a security incident. Does this mean someone has misused or will misuse my data?**

Not necessarily. To date, the City of Whitehall has no evidence that any specific information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and let you know that we continue to take significant measures to protect your information. The purpose of the letter was to make you aware of the incident at the City of Whitehall and provide you with guidance on what you can do to further protect yourself.

**(5) Has any unauthorized person used my information?**

To date, City of Whitehall has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and let you know that we continue to take significant measures to protect your information.

**(6) Who is affected by this incident?**

A limited number of individuals were provided written notice of this incident.

**(7) What information of mine was involved?**

The notice letter that you received specifies which of your information could have been impacted. The information potentially impacted varies from person to person and I do not have the ability to tell you anything more than what your notice letter told you.

**(8) Have you notified law enforcement?**

Yes, we have notified law enforcement officials about this incident.

**(9) Was there a delay in notification of this incident?**

There has been no delay in notification. Upon learning of the access, City of Whitehall commenced a prompt and thorough investigation in consultation with external cybersecurity professionals. The investigation determined certain personal data may have been accessible to unauthorized parties. Thereafter the City of Whitehall worked to provide notice to potentially impacted individuals as quickly as possible.

**(10) What has the unauthorized person done with my information?**

To date, City of Whitehall has no evidence that any individual information has been specifically misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and let you know that we continue to take significant measures to protect your information.

**(11) As a result of this incident, will I become a victim of identity theft?**

Not necessarily. To date, the City of Whitehall has no evidence individual information has been specifically misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and let you know that we continue to take significant measures to protect your information.

**(12) What is City of Whitehall doing in light of this incident?**

Upon learning of this issue, City of Whitehall commenced a prompt and thorough investigation. The City of Whitehall is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. The City of Whitehall also implemented additional safeguards. We will continue to evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

**(13) Does City of Whitehall have any reports of actual misuse of the information as a result of this incident?**

To date, the City of Whitehall has no evidence that individual information has been specifically misused. Nevertheless, out of an abundance of caution, we want to make

you aware of the incident and let you know that we continue to take significant measures to protect your information.

**(14) How do I know if my information was involved in this incident?**

The City of Whitehall has notified those potentially affected via U.S. Mail. If you did not receive a notice letter and you think you may be impacted, please provide your full name and address, and I will confirm whether your information may have been compromised as a result of this incident.

**(15) Why did I <u>not</u> receive a notice about this incident?**

The City of Whitehall provided notice via U.S. Mail to all those potentially impacted to the extent it had a last known home address. If you did not receive a notice letter but you think you may be impacted, please provide your full name and I will confirm whether your information may have been compromised as a result of this incident.

**(16) What can I do to protect myself?**

The City of Whitehall suggests you consider taking the following steps:

- Enroll in the credit monitoring services offered at no cost to you. Instructions to enroll are in the letter you received.
- You should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.
- You may consider placing a fraud alert and/or security freeze on your credit file.
- You may order a free credit report.

**(17) Is City of Whitehall providing credit monitoring services?**

Yes, City of Whitehall is offering you complimentary identity theft protection services through IDX.

**(18) How do I enroll in the credit monitoring product and what is included?**

For further information on IDX identity protection, including instructions on how to activate your one-year membership, please see the additional information provided in your letter.

**(19) Can City of Whitehall just register me in the credit monitoring product?**

Unfortunately, City of Whitehall cannot register for you. You must enroll yourself online (or over the phone) using the Activation Code in your notice letter if you received one.

**(20) How long do I have to enroll in the credit monitoring product?**

You can sign up for this service anytime between now and **t**he date listed in your notification letter. Your activation code is also in your notification letter.

**(21) What is a fraud alert?**

A fraud alert tells creditors to contact you personally before they open any new accounts.

**(22) How do I place a fraud alert on my account?**

In order to place a fraud alert, you will need to call any one of the three major credit bureaus (as soon as one credit bureau confirms your fraud alert, they will notify the others to place fraud alerts). Alternatively, you may file the Fraud Alert online.

***Equifax***
P.O. Box 105069
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

***Experian***
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

***TransUnion LLC***
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

**(23) How long does a fraud alert last?**

An initial fraud alert lasts 1 year and it is free; you may then renew the fraud alert.

**(24) Will a fraud alert stop me from using my credit cards?**

No. A fraud alert will not stop you from using your credit cards or other accounts.

**(25) Can I still apply for a credit card after I place a fraud alert on my credit report?**

Yes, but the verification process may be more cumbersome. Potential creditors will receive a message alerting them to the possibility of fraud and that creditors should re-verify the identity of a person applying for credit.

**(26) How do I place a Security Freeze on my credit files and how much does it cost?**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

***Equifax Security Freeze***
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-

***Experian Security Freeze***
P.O. Box 9554
Allen, TX 75013

***TransUnion Security Freeze***
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze

| | | |
|---|---|---|
| report-services/credit-freeze/<br>(888)-298-0045 | http://experian.com/freeze<br>(888) 397-3742 | (888) 909-8872 |

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

**(27) What should I do if I find suspicious activity on my credit reports or have reason to believe my information is being misused?**

Promptly call your local law enforcement agency and file a police report. Get a copy of the police report, as many creditors will want the information it contains to absolve you of fraudulent debts. You may also file a complaint with the FTC at www.ftc.gov/idtheft or reach the FTC at 1-877-IDTHEFT (1-877-438-4338) or 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

**(28) When I called to place a fraud alert, they asked for my Social Security number. Is this ok?**

Yes. The credit bureaus will indeed ask for your Social Security number and other personal information to verify your identity and avoid sending any credit report or correspondence to the wrong individual. However, the City of Whitehall cautions against you providing any information to any entity or person *contacting you directly* asking for your personal information.

**(29) How do I obtain a free credit report?**

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

**(30) I lost my notification. Can you provide a new one to me?**

Yes. Please confirm your name and address, and the City of Whitehall will ensure that you receive another notification if you are confirmed to be potentially impacted.

**(31) Is this letter legitimate? Is it a scam?**

I can assure you the letter is legitimate. Safeguarding information is a top priority for the City of Whitehall who wants to make you aware of the situation and provide you with guidance on how you can protect yourself.

**(32) Do I have any legal recourse?**

Unfortunately, the City of Whitehall is not in a position to provide any legal advice related to the incident.

**(33) Will we receive any additional information or update?**

The letter sent to you is the only information you will receive.

**(34) The individual this letter is addressed to is deceased. What should I do?**

Please provide your name and contact information and a representative will contact you with information you can use to protect the estate.

**(35) I have additional questions that cannot be answered. What should I do?**

Please provide me with your full name and contact information and we will contact you within forty-eight (48) hours during business hours.

**(36) What is IDX?**

IDX is a service provider to the City of Whitehall and is handling this incident response line on the City's behalf.