



July 24, 2020

Sent via email: SecurityBreach@atg.wa.gov

Office of the Washington State Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Security Incident Notification

Dear Attorney General Ferguson:

This letter is to inform you of an incident involving the unauthorized access of personal information contained in one or both of City of Redmond databases (attackwa.org or pnwfraud.org), both of which were operated by Netsential.com. These databases were a part of a nation-wide data hack into Netsential systems known as the "Blue Leaks" hack, which affected over 200 law enforcement agencies across the country. Netsential reported this hack on June 22, 2020. On June 26, 2020, the City of Redmond discovered that its attackwa.org and pnwfraud.org databases were among the databases affected by this hack. The Blue Leaks data breach is currently under investigation by the Federal Bureau of Investigation (FBI).

The attackwa.org database has been live since January 2018 and is used by both public and private law enforcement partners to create and distribute information amongst various police departments pertaining to automobile-related crimes. There are a variety of documents shared among partner organizations, including other police departments, in this database. Breached information from this database may have included the following personal information: full name or partial name and dates of birth. The breach may also have included addresses; photographs (including booking photos); and, if applicable, prior criminal history and license plate numbers/VIN. In six instances the database also contained social security numbers, driver's license numbers, and/or state ID numbers. The database did not store any financial information such as credit card numbers or financial account numbers. For users of the databases the first and last name, position, department, work contact information, and user name or email address in combination with a password or security questions and answers may have been breached.

We believe approximately 2,851 individuals (the majority of which are Washington residents) in the attackwa.org or pnwfraud.org database may have had personal information, as that term is defined in RCW 42.56.590, breached as a result of this hack. Upon immediate discovery of the breach we contacted the users of attackwa.org and pnwfraud.org via email to instruct them on security measures and to change their username and password. The pnwfraud.org did not contain any personal information of individuals who were not users of the database. Additionally, on June 25, 2020, the City of Redmond issued a press release pertaining to the breach. Samples of the notification letters, including a secondary press release with more details about the breach, are enclosed with this letter.

We have requested (and received confirmation) that Netsential.com has deleted all of the City of Redmond information from its databases and servers. Further, we have discontinued any use of the Netsential.com services. For questions or more information, please contact the City of Redmond at police@redmondwa.gov or (425) 556-2581.

Sincerely,

A handwritten signature in black ink that reads "Darrell Laine". The signature is written in a cursive style with a large, prominent initial "D".

Chief of Police



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

***RE: Important Security Notification
Please read this entire letter.***

Dear <<Name 1>>:

This letter is to inform you of an incident involving the unauthorized access of your personal information. Your personal information was contained in the City of Redmond database attackwa.org, which was operated by Netsential.com. This database was a part of a nation-wide data hack into Netsential systems known as the “Blue Leaks” hack, which affected over 200 law enforcement agencies across the country. Netsential reported this hack on June 22, 2020. On June 26, 2020, the City of Redmond discovered that its attackwa.org database was among the databases affected by this hack. The Blue Leaks data breach is currently under investigation by the Federal Bureau of Investigation (FBI).

The attackwa.org database has been live since January 2018 and is used by both public and private law enforcement partners to create and distribute information amongst various police departments pertaining to automobile-related crimes. There are a variety of documents shared among partner organizations, including other police departments, in this database. Breached information from this database may have included the following personal information: full name or partial name and dates of birth. The breach may also have included addresses; photographs (including booking photos); and, if applicable, prior criminal history and license plate numbers/VIN. Though the database can maintain social security numbers, driver’s license numbers, and state ID numbers, there is no evidence that your social security number, driver’s license number, or state ID number were stored in it. Further, the database did not store any financial information such as credit card numbers or financial account numbers.

Your personal information having been stored in attackwa.org (and your subsequent receipt of this letter) does not necessarily mean you are, or were, a suspect in a crime, as this database also included victim and witness information.

If you are concerned about identify theft, we recommend that you contact one of three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries:

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

Experian (888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion (800) 916-8800
www.transunion.com
P.O. Box 2000
Chester, PA 19022-2000

We take our role in safeguarding your personal information very seriously and deeply apologize for this incident. We continue to discuss additional measures that we as a municipality can adopt to ensure the highest level of security for personal information. For questions or more information, please contact the City of Redmond Police Department at police@redmond.gov or (425) 556-2581.

Sincerely,

A handwritten signature in cursive script that reads "Darrell Laue".

Chief of Police

We only use cookies that are necessary for this site to function, and to provide you with the best experience. Learn more in our [Cookie Statement](#). By continuing to use this site, you consent to the use of cookies.



Receive Updates



PRESS RELEASE: City Aware of Netsential.com Data Breach

City of Redmond Washington sent this bulletin at 07/24/2020 09:29 AM PDT

City of Redmond
Press Release



City Aware of Netsential.com Data Breach

EFFECTIVE IMMEDIATELY

July 24, 2020

CONTACT

Public Information Officer

police@redmond.gov

425-556-2581

Redmond, WA – The City of Redmond is aware of a security/data incident related to “attackwa.org” which was operated by Netsential.com. This database was a part of a nation-wide data hack into Netsential systems known as the “Blue Leaks” hack, which affected over 200 law enforcement agencies across the country. Netsential reported this hack on June 22, 2020. On June 26, 2020, the City of Redmond discovered that its attackwa.org database was among the databases affected by this hack. The Blue Leaks data breach is currently under investigation by the Federal Bureau of Investigation (FBI).

The attackwa.org database has been live since January 2018 and is used by both public and private law enforcement partners to create and distribute information amongst various police departments pertaining to automobile-related crimes. There are a variety of documents shared among partner organizations, including other police departments, in this database. Breached information from this database may have included the following personal information: full name or partial name and dates of birth. The breach may also have included addresses; photographs (including booking photos); and, if applicable, prior criminal history. For all but a handful of individuals, the database did not contain social security numbers, driver’s license numbers, and state ID numbers. Further, the database did not store any financial information such as credit card numbers or financial account numbers.

Individuals whose personal information was stored in attackwa.org are not necessarily a suspect in a crime, as this database also included some victim and witness information. Individuals who are concerned about identify theft, are encouraged to contact one of three

national credit reporting agencies for the purpose of requesting a copy of their credit report or for general inquiries:

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

Experian (888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion (800) 916-8800
www.transunion.com
P.O. Box 2000
Chester, PA 19022-2000

The City of Redmond takes its role of safeguarding personal information very seriously and apologizes for this incident. We continue to discuss additional measures that we as a municipality can adopt to ensure the highest level of security for personal information. For questions or more information, please contact the City of Redmond Police Department at police@redmond.gov or (425) 556-2581. This press release is available on www.redmond.gov/PressReleases.

###



City of Redmond
www.redmond.gov
Email: communications@redmond.gov
15670 NE 85th St, Redmond WA 98073

Follow us:



Don't want to receive this type of email? [Change your email preferences.](#)

Having trouble viewing this email? [View it as a Web page.](#)

 **SHARE**

The City of Redmond assures that no person shall, on the grounds of race, color, national origin, or gender, as provided by Title VI of the Civil Rights Act of 1964 and the Civil Rights Restoration Act of 1987, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity. For more information about Title VI, please visit redmond.gov/TitleVI.

Powered by



[Privacy Policy](#) | [Cookie Statement](#) | [Help](#)



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

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

<<Country>>

<<Date>>

***RE: Important Security Notification
Please read this entire letter.***

Dear <<Name 1>>:

This letter is to inform you of an incident involving the unauthorized access of your personal information. Your personal information was contained in the City of Redmond database attackwa.org which was operated by Netsential.com. This database was a part of a nation-wide data hack into Netsential systems known as the “Blue Leaks” hack, which affected over 200 law enforcement agencies across the country. Netsential reported this hack on June 22, 2020. On June 26, 2020, the City of Redmond discovered that its attackwa.org database was among the databases affected by this hack. The Blue Leaks data breach is currently under investigation by the Federal Bureau of Investigation (FBI).

The attackwa.org database has been live since January 2018 and is used by both public and private law enforcement partners to create and distribute information amongst various police departments pertaining to automobile-related crimes. There are a variety of documents shared among partner organizations, including other police departments, in this database. Breached information from this database may have included the following personal information: full name or partial name, dates of birth, social security number, driver’s license number, and Washington State ID Number. The breach may also have included addresses; photographs (including booking photos); and, if applicable, prior criminal history and license plate numbers/VIN. However, the database did not store any financial information such as credit card numbers or financial account numbers.

Your personal information having been stored in attackwa.org (and your subsequent receipt of this letter) does not necessarily mean you are, or were, a suspect in a crime, as this database also included victim and witness information.

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: 10/17/2020. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by 10/17/2020. Be prepared to provide engagement number <<engagement #>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

You may also contact the other two national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries:

Equifax (800) 685-1111

www.equifax.com

P.O. Box 740241

Atlanta, GA 30374

TransUnion (800) 916-8800

www.transunion.com

P.O. Box 2000

Chester, PA 19022-2000

We sincerely apologize for this incident and regret any inconvenience it may cause you. We continue to discuss additional measures that we as a municipality can adopt to ensure the highest level of security for personal information. For questions or more information, please contact the City of Redmond Police Department at police@redmond.gov or (425) 556-2581.

Sincerely,

A handwritten signature in black ink that reads "Darrell Laue". The signature is written in a cursive, slightly slanted style.

Chief of Police

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

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

<<Country>>

<<Date>>

RE: Supplement to Security Notification – Netsential.com Breach

Dear <<Name 1>>:

This letter is a supplement to the prior security notification the City of Redmond Police Department emailed you on June 24, 2020, regarding the “attackwa.org” and “pnwfraud.org” security incident. As noted previously within our original notice encouraging you to change your password(s), we have been investigating the scope of the incident, which Netsential.com reported on June 22, 2020. As of June 26, we have confirmed that the “attackwa.org” and “pnwfraud.org” databases were, in fact, a part of the Netsential.com breach (commonly referred to as the “Blue Leaks”). This data breach is currently under investigation by the Federal Bureau of Investigation.

We have reason to believe that the breached information from the databases may have included your first and last name, position, department, work contact information, and importantly your user name or email address in combination with a password or security questions and answers that would permit access to the databases. Out of an abundance of caution, though the passwords were encrypted and hashed, we believe that this supplemental notification is necessary.

If you have used the same login credentials for other databases, we encourage you to change those passwords immediately. To further safeguard our databases, we have since ceased working with Netsential.com, and have requested that they purge all of our data from their records. We will continue to discuss additional measures we can adopt to ensure the highest level of security for personal information.

The data breach did not involve any financial information. However, if you are concerned about identity theft, we recommend that you contact one of three national credit reporting agencies to request a copy of your credit report or for general inquiries:

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

Experian (888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion (800) 916-8800
www.transunion.com
P.O. Box 2000
Chester, PA 19022-2000

If you have any questions, or would like more information, please contact the City of Redmond Police Department at police@redmond.gov or (425) 556-2581.

Sincerely,

A handwritten signature in black ink that reads "Darrell Laune". The signature is written in a cursive, flowing style.

Chief of Police