



7 Bulfinch Place  
Boston, MA 02114

RECEIVED  
DEC 03 2020  
CONSUMER PROTECTION

December 1, 2020

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Security Incident

To Whom it May Concern:

I am writing on behalf of WHDH-TV, an independent television station licensed in Boston, Massachusetts, to inform you that notice is being sent to forty (40) New Hampshire residents regarding a recent security incident in which certain of their personal information was accessed and copied without authorization.

**I. Nature of the Security Incident.**

In August 2020, WHDH-TV was subject to a ransomware attack that corrupted many of its computer systems and records. WHDH-TV was able to restore the impacted systems and records from backups, and its investigation did not reveal any theft of personal information. News of the attack was shared with employees at the time.

On October 10, 2020, WHDH-TV became aware of additional information suggesting that the perpetrators of the attack had also stolen certain WHDH-TV records during the incident. WHDH-TV promptly launched an investigation focusing on the records at issue, hired a forensics firm to assist in further understanding the incident based on the new information, and notified law enforcement. On October 25, 2020, two days after the specific records at issue were identified, the investigation confirmed that the perpetrators copied a WHDH-TV database containing various records, some of which included current and former employee names, Social Security numbers, and in some cases, dates of birth. The perpetrators posted the WHDH-TV records on a black market website as part of an attempted extortion scheme.

**II. Number of Residents Affected and Notified.**

Forty (40) New Hampshire residents have been identified as affected by the incident. Notice to the New Hampshire residents is being sent via first class mail on December 2, 2020. Notification was not delayed due to a law enforcement investigation.

**III. Steps WHDH-TV has Taken to Address the Incident.**

We take our responsibility to protect our employees' privacy seriously. We regret that this incident occurred, and have implemented the following measures to help mitigate its impact and to prevent a similar incident from reoccurring:

- WHDH-TV arranged to have Experian help protect the affected individuals from identity theft. Specifically, WHDH-TV has made available to the affected individuals, free of charge, 24 months of active credit monitoring, identity theft insurance, and identity repair services. Please see the enclosed copy of the notification letter for additional details.
- WHDH-TV has provided an explanation of additional steps that affected individuals may consider taking, free of charge, to further protect themselves, including checking credit reports, utilizing fraud alert services and placing a security

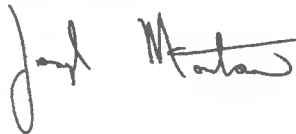
December 1, 2020

freeze on credit reports, as further explained in the enclosed copy of the notification letter.

- WHDH-TV is providing the individuals with a toll-free telephone number that they may call with questions about the incident, as further explained in the enclosed copy of the notification letter.
- As a courtesy, WHDH-TV is also providing the above services and resources (free of charge) to those WHDH-TV employees whose personal information was not involved in the incident.
- WHDH-TV deployed VMware's cloud native Carbon Black Endpoint Detection and Response tool to all available WHDH-TV endpoints, including servers, laptops, and workstations. The tool provides multiple endpoint security capabilities including Next Generation Anti-Virus, containment and remediation, managed detection, and threat hunting capabilities, allowing the identification of active threats, preventing attackers from using legitimate tools, running on demand queries, and remotely remediating identified concerns.
- WHDH-TV has taken active steps to help prevent a similar incident from occurring in the future, including implementing additional security awareness training and conducting a post-incident review to assess its response to the incident and to identify areas where WHDH-TV policies and practices can be improved. WHDH-TV will improve its policies and practices based on such assessment and best practices.

Please contact me if you have any questions.

Sincerely yours,



Joseph Montano  
Director of Administration and Finance  
WHDH-TV/WLVI-TV  
7 Bulfinch Place  
Boston, MA 02114  
Office: (617) 725 – 0736  
Cell: (617) 921 – 6089

Enclosure

#80636037\_v2



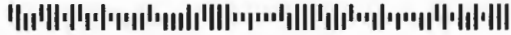
Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

December 2, 2020

G0110-L01-0000001 T00017 P003 \*\*\*\*\*ALL FOR AADC 123



SAMPLE A SAMPLE - L01 INCIDENT  
APT ABC  
123 ANY ST  
ANYTOWN, US 12345-6789



Dear Sample A Sample,

We are writing to notify you of a security incident involving your personal information. In August 2020, WHDH-TV was subject to a ransomware attack that corrupted many of its computer systems and records. WHDH-TV was able to restore the impacted systems and records from backups, and its investigation did not reveal any theft of personal information. News of the attack was shared with employees at the time.

On October 10, 2020, WHDH-TV became aware of additional information suggesting that the perpetrators of the attack had also stolen certain WHDH-TV records during the incident. WHDH-TV promptly launched an investigation focusing on the records at issue, hired a forensics firm to assist in further understanding the incident based on the new information, and notified law enforcement.

The investigation has now confirmed that the perpetrators copied a WHDH-TV database containing various records, some of which included current and former employee names, Social Security numbers, and in some cases, dates of birth. The perpetrators posted the WHDH-TV records on a black market website as part of an attempted extortion scheme. You are receiving this letter because your information was included in the WHDH-TV records at issue.

We would like to emphasize that, based on the information we have to date, we are not aware of any instances of fraud or identity theft resulting from the incident. Nevertheless, as a precautionary measure, we have arranged to have Experian provide its Experian IdentityWorks<sup>SM</sup> to you, free of charge, for the next 24 months beginning from the date of this letter. Experian IdentityWorks consists of several services, including active credit monitoring, identity restoration services, and Experian's ExtendCARE<sup>TM</sup> support.

**In order to be eligible to receive Experian IdentityWorks, you must enroll no later than February 28, 2021.** You may enroll via the IdentityWorks website (<https://www.experianidworks.com/credit>) using your activation code . If you have questions about Experian IdentityWorks, would like to enroll over the phone, or need other assistance, please contact Experian's customer care team at (866) 274-5767 by February 28, 2021 (your code will not work after this date), and be prepared to provide your engagement number DB24066 as proof of eligibility for the Identity Restoration services by Experian. Included below is additional information from Experian about IdentityWorks and the services made available to you.

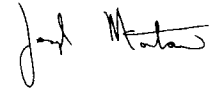
We have also included with this letter an explanation of additional steps you may consider taking to further protect yourself, including checking your credit reports, utilizing fraud alert services, and placing a security freeze on your credit reports, all at no charge. Experts recommend, as a general consumer protection measure, that you periodically review your credit report and account statements, even if you do not initially find suspicious activity.



We take our responsibility to protect our employees' privacy seriously. We regret that this incident occurred, and have implemented measures to help prevent an incident like this from happening again. Going forward, we will continue to look for ways to improve the security of our systems.

If you have any questions, please call (866) 274-5767 toll-free Monday through Friday from 8 am to 10 pm Central, or Saturday and Sunday from 10 am to 7 pm Central (excluding major U.S. holidays).

Sincerely,



Joseph Montano  
Director of Administration and Finance  
WHDH-TV/WLVI-TV

## IDENTITY THEFT PRECAUTIONS

### Free Credit Report

The Fair Credit Reporting Act requires each of the three nationwide credit reporting agencies (Equifax, Experian, and TransUnion) to provide you annually, upon request, with a free copy of your credit report. Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by phone at 1-877-322-8228.

You can also request your free credit report by completing the request form at: [www.annualcreditreport.com](http://www.annualcreditreport.com), and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

### Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major credit reporting agencies listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file.

**Equifax®**  
P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-685-1111  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Experian**  
P.O. Box 9701  
Allen, TX 75013-9701  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion®**  
P.O. Box 1000  
Chester, PA 19016-1000  
1-800-888-4213  
<https://www.transunion.com/fraud-alerts>

### Security Freeze

You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Consumers may place a security freeze on their credit reports at no charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

Under federal law, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may each charge you to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request by regular, certified, or overnight mail at the addresses below to each of the three major credit reporting agencies: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)). You may also request the security freeze through each of the credit reporting agencies' websites or over the phone:

**Equifax**  
P.O. 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)

**Experian**  
P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016-2000  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)



In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies 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 as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

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.

#### **Further Information**

You may obtain additional information about identity theft (including, a security freeze) by contacting the above or the Federal Trade Commission (FTC) using the contact information below.

**Federal Trade Commission  
Consumer Response Center**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

#### **Additional Information Regarding Experian Services**

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 24 months 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](http://www.ExperianIDWorks.com/restoration).

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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

\* 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.

