Clark Hill

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email:jschwent@clarkhill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

August 5, 2021

**VIA Online Notification Portal**

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Aaron Frey:

We represent NTS Holding Corporation ("NTS") with respect to a security incident involving the potential exposure of certain personally identifiable information described in more detail below. NTS, located in Anaheim, California, is an independent test, inspection, and certification company. NTS is committed to answering any questions you may have about the security incident, its response, and steps taken to minimize the risk of a similar incident in the future.

**1. Nature of security incident.**

On November 2, 2020, NTS experienced a security incident that interrupted access to its systems. As soon as NTS learned of the incident, NTS began an internal investigation and hired independent cybersecurity specialists to help determine what occurred and whether any information was at risk. The cybersecurity specialists determined that an unauthorized actor gained access to certain NTS systems and deployed malware within the environment. The investigation also determined that certain files stored within the NTS network may have been accessed by the unauthorized actor, but forensic investigators were unable to confirm. Out of an abundance of caution, NTS conducted a thorough review of the contents of the files. Because of the volume and types of data potentially at issue, the review of that data took time to complete.

On March 17, 2021, the investigation confirmed that the impacted data included information related to certain individuals. From the review, it appears the data may have included names, dates of birth, Social Security numbers, and financial account information. NTS then expended significant efforts to validate the data and obtain accurate contact information for affected individuals to process notifications. Again, the volume of impacted data caused delays in completing this work. This effort was completed on July 9, 2021.

**2. Number of residents affected.**

One (1) Maine residents may have been affected and were notified of the incident. A notification letter was issued to all impacted on August 5, 2021 via regular mail. A copy of the template notification letter is enclosed.

**3. Steps taken relating to the incident.**

Since the incident, NTS has taken steps to minimize the risk of this happening in the future, including but not limited to resetting all passwords and fully deploying advanced endpoint threat detection and monitoring on all network-connected systems. Credit monitoring and identity protection services through IDX were offered at no cost.

**4. Contact information.**

NTS takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Very truly yours,

CLARK HILL

Jason M. Schwent
Senior Counsel

(Enclosure)

2125 East Katella Avenue
Suite 250
Anaheim, CA 92806

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

August 5, 2021

**Notice of Data Security Incident**

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident experienced by NTS Holding Corporation ("NTS") that may have impacted your personal information. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

**What happened:**

On November 2, 2020 we discovered a data security incident that disrupted access to our network. As part of our response process, we initiated our business continuity protocols and engaged an independent computer forensic investigator to help us determine what occurred and whether any information was at risk. The forensic investigators found that an unauthorized actor gained access to certain NTS systems and files stored on our network but were unable to confirm whether the information was accessed or viewed. Out of an abundance of caution, NTS conducted a thorough review of the contents of the files. On March 17, 2021, the investigation confirmed that the impacted data included information related to certain individuals. NTS then worked to validate the data and obtain accurate contact information to process notifications. The list was finalized, and we determined that your information may have been impacted by this incident.

**What information was involved:**

While there is no evidence that the files were accessed or viewed, the investigation concluded that the files may have contained your first and last name, Social Security number, financial account information, and date of birth.

**What we are doing:**

NTS takes this incident and the security of your personal information seriously. We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have implemented additional controls for all types of remote access to our systems and performed a global password reset. We have also notified and are cooperating with law enforcement.

In addition, while we are not aware of any misuse of your information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you, as a precautionary measure.

We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring*** services at no charge. These services provide you with alerts for <<length of service>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

* Services marked with an "*" require an internet connection and valid e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**What you can do:**

For 90 days from the date of this letter, representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern time to assist you with questions regarding this incident. Please call 877-264-9632 with any questions you may have and supply the specialist with your unique code listed below.

**How to Enroll in services: You must enroll online**

To enroll in free Credit Monitoring* services, please log on to https://secure.identityforce.com/benefit/ntsholdings and follow the instructions. When prompted, please provide the following unique code to receive services: <CODE HERE.> Please note the deadline to enroll is November 5 2021.

For guidance with the services, or to obtain additional information about these services during or after enrollment, please call the help line 877-264-9632 and supply the specialist with your unique code.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

**For more information:**

You will find additional information in the enclosed document. Also, you will need to reference the enrollment code within this letter when calling or enrolling online, so please do not discard this letter.

Please call 877-264-9632 Monday through Friday from 9 am - 9 pm Eastern time for assistance or for any additional questions you may have.

Your trust is a top priority for us, and we sincerely apologize for any concern or inconvenience this may cause you.

Sincerely,

Dave Robertson
Chief Human Resources Officer
NTS Holding Corporation

* Services marked with an "*" require an internet connection and valid e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

## Additional Information

**For residents of *Hawaii, Michigan, Missouri, New Mexico, Virginia, Vermont,* and *North Carolina*:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

**For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, Washington,* and *West Virginia*:** It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

**Equifax**
P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

**Experian**
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

**TransUnion**
P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**For residents of *Iowa*:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of *Colorado, Maryland, Illinois, North Carolina,* and *Rhode Island*:** You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Maryland Attorney General**
Consumer Protection Div.
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

**North Carolina Attorney General**
Consumer Protection Div.
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
919-716-6000
www.ncdoj.com

**Rhode Island Attorney General**
Consumer Protection Div.
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

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

**For residents of *Rhode Island*:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident. There were nine Rhode Island residents impacted by this incident.

**For residents of *California*:** You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

**For residents of *District of Columbia*:** You may obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia by visiting https://oag.dc.gov/consumer-protection, emailing consumer.protection@dc.gov, calling (202) 442-9828, or mailing Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW Washington, DC 20001.

**For residents of *New York*:** You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-

* Services marked with an "*" require an internet connection and valid e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

**For residents of *Oregon***: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

**For residents of all states:** More information can also be obtained by contacting the Federal Trade Commission listed above.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via each credit bureau's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below. As of September 21, 2018, fraud alerts will now last one year, instead of 90 days. Fraud alerts will continue to be free and identity theft victims can still get extended fraud alerts for seven years.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, each credit reporting agency has a dedicated web page for security freezes and fraud alerts or you can request a freeze by phone or by mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request may also require a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Effective September 21, 2018, placing a freeze on your credit report is now free for all United States citizens.

**Equifax**
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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

**TransUnion**
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/credit-freeze

* Services marked with an "*" require an internet connection and valid e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.