September 26, 2022

Via US Mail
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

RE: Northern Data Systems Security Incident

Dear Sir/Madam:

I am writing to notify you that Northern Data Systems, Inc. (NDS) suffered a security incident that resulted in the potential unauthorized access of a limited subset of personal information of one New Hampshire resident. As we are a managed services provider, we maintain files for other companies rather than specific individuals. So, the files that were affected contained data our customers had collected from other individuals.

NDS was the target of a ransomware attack in May 2022. The threat actor gained access on May 6, 2022, and we discovered the attack on May 13, 2022. We reported the incident to law enforcement and promptly engaged outside counsel, who in turn engaged a leading forensic/cybersecurity firm to assist in the investigation. As part of our response to the incident, we quickly contained the threat, rebuilt the relevant systems from backups, and took measures to secure our network against a similar attack. We also made contact with the threat actor—who claimed to have exfiltrated data from our environment. We worked with industry experts to validate the exfiltration claim to the extent we could and then identify the potentially affected files. Once we identified those files, we provided them to a data review firm to assess what information they contained. We received those results in June and began assessing potential notification obligations. We later determined that the threat actor publicly disclosed the exfiltrated data. In order to ensure all relevant individuals were identified, additional time was needed to retrieve the disclosed data and compare it against previously reviewed files. With that process now complete, we have been verifying addresses and coordinating with our clients on providing the required notices.

We have reason to believe that the threat actor potentially accessed digital, non-encrypted personal information of one New Hampshire resident. The New Hampshire resident had the following information potentially affected: full name, contact information, and Social Security number. Consistent with our obligations under state law, on September 26, 2022, we provided written notice to the affected individual informing them that some of their personal information may have been affected.

We have attached a template of the notice we provided to the affected New Hampshire resident. In that letter, we provided the individual with one year of Experian IdentityWorks, a credit-monitoring service, because their Social Security number may have been affected.

NORTHERN DATA SYSTEMS, INC.
362 U.S. ROUTE ONE ❖ PO. BOX 66738 ❖ FALMOUTH, ME 04105
TEL (207) 781-3236
FAX (207) 781-3226

Since the incident, as noted above, we have taken a variety of measures in response. We have changed/strengthened passwords, started the process of implementing multifactor authentication, adopted new technical safeguards, and modified our software.

Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,

Mark Stevens
Chief Executive Officer

NORTHERN DATA SYSTEMS, INC.
362 U.S. ROUTE ONE ◆ PO. BOX 66738 ◆ FALMOUTH, ME 04105
TEL (207) 781-3236
FAX (207) 781-3226

NORTHERN DATA SYSTEMS, INC.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing on behalf of Northern Data Systems to inform you that we suffered a security incident that potentially affected your personally identifiable information. We provide computing services, including data hosting, for other companies, and your personally identifiable information was collected by one of our customers and maintained in the environment we host for that customer. While monitoring our network, we discovered on May 13, 2022, that an unauthorized third party had gained access to a portion of our environment. We promptly began working with third-party experts to investigate and respond to the incident. And we are now providing you this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party gained access to part of our environment. During the course of our experts' investigation, they identified the files that may have been affected. On May 25th, we engaged a data review firm to comb through that data and identify what information was in the files. That process takes some time. We received the data review firm's results on July 25th. Since then, we have been assessing who to notify and locating correct contact information for those involved so that we can provide them notice.

WHAT INFORMATION WAS INVOLVED

This incident may have exposed some of your personally identifiable information. The affected data may include details such as your name, contact information, Social Security or driver's license number, and financial information (such as a bank account number).

WHAT WE ARE DOING

We worked with third-party experts to investigate and respond to the incident, and we are further securing our systems to protect your information. Additionally, on the next page, you will find details on how to activate the complimentary credit monitoring we are providing as well as advice regarding other measures you can take to protect yourself against fraud or identity theft.

FOR MORE INFORMATION

Should you have any questions, you can contact us at [TFN], Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Mark Stevens
Chief Executive Officer

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you enroll by: <<b2b_text_6 (date)>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your activation code: **<<Activation Code s_n>>**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-890-9332 by <<b2b_text_6 (date)>>, and provide them engagement number <<b2b_text_1 (engagement #)>>.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

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

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

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

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

New York Attorney General
The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.