

May 2, 2023

VIA E-Mail

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@ag.iowa.gov

Re: Notice of Data Incident

Dear Sir or Madam:

We are writing on behalf of our client, NextGen Healthcare, Inc., to inform you of a data incident.

On March 30, 2023, NextGen was alerted to suspicious activity on its NextGen Office system. In response, NextGen launched an investigation with the help of leading third-party forensic experts. NextGen also took measures to contain the incident, including by resetting passwords, and further reinforcing the security of our systems. NextGen also contacted law enforcement and has been cooperating with them since.

Based on its in-depth forensic investigation to date, NextGen determined that an unknown third-party gained unauthorized access to a limited set of electronically stored personal information between March 29, 2023 and April 14, 2023. NextGen also determined that the unknown third-party accessed the NextGen Office system by using NextGen client credentials that appear to have been stolen from sources or incidents unrelated to NextGen. NextGen performed a detailed analysis and review of the impacted data, and only recently discovered that certain of personal information belonging to Iowa residents was included in the electronic data accessed during the incident. The information impacted included: name, date of birth, address, and social security number. Importantly, NextGen investigation has revealed no evidence to suggest there was any access or impact to any health or medical records or any health or medical data.

From NextGen's investigation, it appears that 14,844 Iowa residents have been impacted by the incident. Notifications to the impacted individuals in Iowa were sent out by U.S. mail on or about April 28, 2023. (A sample copy of that notice is enclosed.) At the same time, NextGen sent out corresponding notification to all of its provider customers who had patients with impacted personal information. NextGen has also notified the three credit bureaus.

Even though NextGen, has no evidence that any personal information has been fraudulently used as a result of this incident, NextGen is offering impacted individuals 24 months of free fraud

May 2, 2023
Page 2

detection monitoring and identity theft protection through Experian's IdentityWorksSM product. Further, in its written notification, NextGen has provided impacted individuals with detailed information regarding additional steps they can take to protect themselves and their personal information.

We assure you that our client, NextGen takes this issue, and the privacy and security of personal information, very seriously. If you have any questions or require further information, please feel free to contact me at krollins@sheppardmullin.com or (212) 634-3077.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kari M. Rollins". The signature is fluid and cursive, with a long horizontal stroke at the end.

Kari M. Rollins
for SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

SMRH:4856-6194-5093.2
Enclosure



Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 12 *****AUTO**MIXED AADC 460

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



April 28, 2023

Re: Notice of Data Incident

Dear Sample A. Sample:

We are writing to let you know about a security incident involving certain of your personal information. This notice explains what happened, what information may have been affected, what measures we are taking in response, and steps you can take to protect yourself.

Who We Are

NextGen Healthcare, Inc. provides electronic health records and practice management solutions to doctors and medical professionals. In support of the services we provide to your medical professionals, we maintain certain of your personal information on their behalf.

What Happened

On March 30, 2023, we were alerted to suspicious activity on our NextGen Office system. In response, we launched an investigation with the help of third-party forensic experts. We also took measures to contain the incident, including resetting passwords, and contacted law enforcement .

Based on our in-depth investigation to date, supported by our external experts, it appears that an unknown third-party gained unauthorized access to a limited set of electronically stored personal information between March 29, 2023 and April 14, 2023. As a result of our detailed analysis of the information impacted, we recently determined that certain of your personal information was included in the electronic data accessed during the incident. Below we have provided information about what information was involved, what we are doing in response, and what you can do to proactively protect yourself.

What Information Was Involved

The personal information contained in the electronic data accessed during the incident included your name, date of birth, address, and social security number. Importantly, our investigation has revealed no evidence of any access or impact to any of your health or medical records or any health or medical data. Furthermore, there is no evidence to suggest there has been any fraudulent use of the personal information accessed.

What We Are Doing

As noted, as soon as we discovered the suspicious activity, we launched an internal investigation and engaged the assistance of leading forensic experts. At the same time, we took measures to contain the incident, including resetting passwords, and further reinforcing the security of our systems. We also contacted law enforcement, and have been working with them since.



We take this matter very seriously, and in addition to the steps already described, NextGen Healthcare is offering you **24 months of free fraud detection and identity theft protection** through Experian's® IdentityWorksSM product. If you wish to take advantage of these services, activation instructions are below.

What You Can Do

Though we have no evidence that any of your personal information has been fraudulently used, we encourage you to remain vigilant by reviewing your account statements and credit reports closely. At the end of this letter, we have provided you with additional information regarding steps you can proactively take to further protect yourself and your personal information. It describes information about (1) reporting suspicious activity or suspected identity theft, (2) credit reports, (3) fraud alerts, (4) credit/security freezes, (5) your rights under the Fair Credit Reporting Act, and (6) information about taxes. We encourage you to review that additional information.

Free Credit Monitoring and Identity Theft Protection: Even though we have no evidence that your personal information has been fraudulently used, as a precautionary measure, we are offering to provide you with 24 months of free identity monitoring, fraud consultation, and identity theft restoration services through Experian's IdentityWorksSM product. To take advantage of these free services, please follow the steps below:

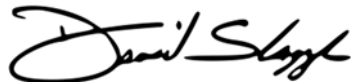
- Ensure that you enroll by **August 31, 2023**. Your code will not work after this date.
- Visit the Experian IdentityWorksSM website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product or need assistance with identity restoration that arose as a result of this incident, please contact Experian's customer care team at **800-984-8279** by August 31, 2023. Please be prepared to provide engagement number **B090760** as proof of eligibility for the identity restoration services by Experian.

For More Information

We take very seriously the security and privacy of your information, and deeply regret any inconvenience this may cause. If you have any questions, please call us at **800-984-8279**, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please be prepared to provide your engagement number **B090760**.

Sincerely,



David Slazyk
Chief Information & Security Officer

Additional Steps You Can Take to Protect Your Personal Information

Report Suspicious Activity or Suspected Identity Theft. If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at www.ftc.gov. You can also contact your state Attorney General (information for some specific AGs is listed below):

- District of Columbia residents may wish to review information provided by the District of Columbia Attorney General on steps to take to avoid identity theft at <https://oag.dc.gov/>, emailing at consumer.protection@dc.gov, calling (202) 442-9828, or by writing to Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001.
- Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us>, by sending an email to idtheft@oag.state.md.us, or by calling 410-576-6491.
- New York residents may wish to review information on security breach response and identity theft prevention and protection information provided by the New York Attorney General at <https://ag.ny.gov/internet/privacy-and-identity-theft> or by calling 1-800-771-7755 and by the New York Department of State, Division of Consumer Protection at <https://dos.ny.gov>, or by calling 800-697-1220.
- North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/>, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, NC 27699.
- Rhode Island resident may wish to review information provided by the Rhode Island Attorney General at <http://www.riag.ri.gov> or by calling 401-274-4400, or by writing to 150 South Main Street, Providence, RI 02903.

Contacting the Internal Revenue Service: If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate. For the IRS, you can use Form 14039 (<https://www.irs.gov/pub/irs-pdf/f14039.pdf>). You can also call them at 800-908-4490 (Identity Theft Hotline). Information on how to contact your state department of revenue to make similar reporting may be found by going to <http://www.taxadmin.org/state-tax-agencies>.

Credit Reports/Fraud Alerts/Credit and Security Freezes: Under federal law, you are entitled to one free copy of your credit report every 12 months. You can request a free credit report once a year at www.annualcreditreport.com, by calling (877) 322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.



In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. There may be a fee for this service based on state law (in MA, there shall be no charge). To put a security freeze on your credit file contact the consumer reporting agencies listed below.

You may contact the three U.S. credit reporting agencies as follows:

Agency	Credit Report Contact	Fraud Alert Contact	Credit/Security Freeze Contact
TransUnion LLC	TransUnion LLC Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016; (800) 888-4213; https://www.transunion.com	TransUnion Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19016; (800) 680-7289; https://www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 160, Woodlyn, PA 19094; (888) 909-8872; https://www.transunion.com/credit-freeze/
Experian	P.O. Box 2002, Allen, TX 75013; (888) 397-3742; https://www.experian.com/consumer-products/free-credit-report.html	Experian, P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/fraud/center.html	P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/freeze/center.html
Equifax Information Services LLC	Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374; (866) 349-5191; https://www.equifax.com/personal/credit-report-services/	Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348-5069; (800) 525-6285; https://www.equifax.com/personal/credit-report-services/	Equifax Information Services LLC, P.O. Box 105788, Atlanta, GA 30348-5788; (888) 298-0045 or (800) 349-9960; https://www.equifax.com/personal/credit-report-services/

Federal Fair Credit Reporting Act rights: You have rights under the federal Fair Credit Reporting Act that include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. More information about your rights is at www.ftc.gov.

IRS Identity Protection PIN: The IRS offers an Identity Protection PIN, which is a six digit number that prevents someone else from filing a tax return using your Social Security number. The Identity Protection PIN is known only to you and the IRS. For more information and to obtain an Identity Protection PIN, please visit the IRS website at <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.