K&L GATES

March 1, 2023

By FedEx

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident – Reventics, LLC

To whom it may concern:

Please be advised that we are legal counsel to Reventics, LLC ("Reventics"). On or about December 15, 2022, Reventics, a revenue cycle management company that partners with healthcare providers, detected certain irregularities in its systems, including a cyber-intruder who encrypted and potentially accessed information on Reventics' servers.

Upon detecting the incident, and to mitigate any potential harm, Reventics immediately took action to secure the affected systems and contain the incident. Reventics also engaged an international cybersecurity and forensic consulting firm to assess the cyber-attack and contain any further threats to its systems, including any systems containing patient information. On or about December 27, 2022, it was determined that unauthorized acquisition of information had occurred. Certain personally identifiable information ("PII") and Protected Health Information ("PHI") protected under HIPAA and state privacy laws was contained on Reventics' systems and was impacted by the breach. In the aftermath of the incident and on an ongoing basis, Reventics' internal teams continue to work diligently with their third-party cybersecurity consultants to further fortify Reventics' systems, including implementing new technical safeguards, revising policies and procedures, and retraining workforce members. Reventics also engaged our firm to assist with notifying law enforcement, preparing regulatory notices, and notifying those individuals who may have been impacted by this incident.

Additionally, to help relieve concerns and restore confidence following this incident, Reventics is offering identity theft protection services to impacted individuals through IDX, a data breach and recovery services expert, at no cost to the individuals. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help affected individuals address and resolve issues if their identity is compromised.

K&L GATES LLP
70 W. MADISON ST. SUITE 3100 CHICAGO IL 60602
T +1 312 372 1121 F +1 312 827 8000 klgates.com

The approximate number of New Hampshire residents affected by the breach is forty-nine (49). Given that Reventics is a Business Associate to various Covered Entities, the state of residence and addresses of the data subjects at issue is not necessarily known to Reventics. Therefore, Reventics first provided substitute notice by way of its website on February 10, 2023. Once Reventics was able to locate and/or procure address information, it began notifying affected New Hampshire residents via U.S. mail on February 24, 2023. A sample copy of the notification letter sent to the affected residents is included with this correspondence.

Very truly yours,

Desirée Moore

REVENTICS
A Provider Engagement Company

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

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

Notice of Data Security Incident

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

We are writing to tell you about a data security incident that may have exposed some of your personal information that we have in our possession because of clinical documentation and reimbursement services we provide to a healthcare provider or providers where you have received care. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On or about December 15, 2022, Reventics, LLC ("Reventics"), a revenue cycle management company that partners with healthcare providers, detected certain irregularities in its systems, including a cyber-intruder who encrypted and potentially accessed information on Reventics' servers. Reventics immediately engaged an international cybersecurity and forensic consulting firm to investigate and assess the cyber-attack and contain any further threats to Reventics' systems, including any systems containing your information. On or about December 27, 2022, it was determined that unauthorized acquisition of information had occurred. Certain personally identifiable information ("PII") and Protected Health Information ("PHI") protected under HIPAA and state privacy laws was contained on Reventics' systems and was impacted by the breach. In the aftermath of the incident and on an ongoing basis, Reventics' internal teams continue to work diligently with their third-party cybersecurity consultants to further fortify Reventics' systems, including implementing new technical safeguards, revising policies and procedures, and retraining workforce members.

What information was involved?

The information that may have been compromised potentially included your first, middle, and last name, address, date of birth, medical record number, patient account number, driver's license and other government issued ID, healthcare provider's name and address, health plan name and health plan ID, clinical data including diagnosis information, dates of services, treatment costs, prescription medicate ons, the numeric codes used to identify services and procedures you received from your healthcare provider, and a brief description of these codes.

What we are doing.

Upon detecting the incident, and to mitigate any potential harm, Reventics immediately took action to secure the affected systems and contain the incident. Reventics then notified other stakeholders, and, as noted above, retained a leading third-party cybersecurity and forensic consultant to investigate the nature and scope of the incident and secure the data environments. Additionally, Reventics engaged an international law firm to assist with notifying law enforcement, preparing regulatory notices, and notifying those who may have been impacted by this incident.

Further, to help relieve concerns and restore confidence following this incident, Reventics is offering identity theft protection services through IDX, a data breach and recovery services expert, at no cost to you. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

Visit **[ ].com** to activate and take advantage of your identity monitoring services.

*You have until **[date]** to activate your identity monitoring services.*

REVENTICS
A Provider Engagement Company

Membership Number: <<Member ID>>

Additional information describing services available to you is included with this letter.

What you can do.

In addition to activating identity monitoring services, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have any questions, please call (833) 753-4765,Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Please have your [membership number] ready. Protecting your information is paramount to us and we hope that the services we are offering to you demonstrate our commitment in this regard.

Sincerely,

[Name]
[Title]
[Company]

REVENTICS
A Provider Engagement Company

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/reventics and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax'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 bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you

REVENTICS
A Provider Engagement Company

will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.