



<<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>> <<last_name>>:

Harbin Clinic, LLC ("Harbin Clinic") is committed to protecting the confidentiality and security of its patients' information. Regrettably, Nationwide Recovery Services, Inc. ("NRS") recently notified Harbin Clinic that a data security incident experienced by NRS may have potentially involved some of your personal and/or health information. NRS is a third-party vendor that has provided debt collection services for delinquent accounts of individuals treated at Harbin Clinic, as well as services related to bankruptcies, lawsuits and patient estate matters. This notice explains the incident and outlines the measures we have taken in response and steps you can take.

What Happened?

It is our understanding that, in July 2024, NRS discovered suspicious activity related to its information technology systems, which resulted in a network outage. NRS indicated that it determined through an investigation there was unauthorized access to the NRS network between July 5, 2024 and July 11, 2024, during which time certain files and folders were illegally copied from NRS's systems by someone without authorization. NRS reported it began a lengthy review to determine what information was contained on the impacted NRS systems and which NRS clients were impacted.

As a result of this review, NRS notified Harbin Clinic in February 2025 that information from Harbin Clinic's patients may have been present on the impacted systems, but it was not yet able to identify which individuals had been impacted. In March, NRS provided Harbin Clinic with a list of individuals whose information may have been impacted by the incident.

What Information Was Involved?

We are notifying you because NRS determined that some of your information may have been present on its impacted systems. According to NRS, this information may have included your name, address, Social Security number, date of birth, financial account information, guarantor information and/or medical-related information.

What Are We Doing?

NRS reported that it has no evidence to suggest there has been identify theft or fraud related to this incident. However, we wanted to notify you of this incident and assure you we take this very seriously. NRS reported that, upon becoming aware of this incident, it immediately took steps to confirm the security of its systems and to determine what information was potentially impacted, including notifying law enforcement. NRS also said it has implemented additional cybersecurity measures and reviewed existing security policies to protect against similar incidents moving forward.

While Harbin Clinic systems were not affected by this breach, Harbin Clinic has also taken the following steps to address the situation and prevent future occurrences:

- Harbin Clinic immediately blocked NRS's access to Harbin Clinic systems until a forensic investigation firm determined the threat had been eradicated from the NRS network.
- Harbin Clinic conducted a review of its own systems to ensure no indicators of compromise were present in its own network.
- Harbin Clinic engaged its privacy and cybersecurity teams to conduct an investigation of the incident and work with NRS to determine the scope of the breach and identify potentially impacted Harbin Clinic patients.

We are continuing to monitor, evaluate and enhance our security systems and controls, as appropriate, to minimize the risk of similar incidents in the future.

What Can You Do?

Unfortunately, cyber-attacks can and do happen every day all around the world. We encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity to your financial institution immediately. Federal regulatory agencies recommend remaining vigilant for 12 to 24 months following a potential exposure of personal information. The enclosed reference guide includes additional information on general steps you can take to monitor and protect your personal information.

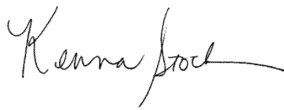
To help protect your identity, we are offering a complimentary 24 month membership of Kroll identity monitoring. To activate your membership and start monitoring your personal information, please follow the steps outlined in the attached addendum.

Other Important Information.

We are truly sorry this happened and apologize for any concern or inconvenience this incident may cause.

Should you have any further questions or would like additional information, please visit <https://harbinclinic.com/NRSnotice> or call toll-free (866) 408-3081. The call center is here to help you and is open Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "Kenna Stock", with a stylized flourish at the end.

Kenna Stock
President & Chief Executive Officer
HIPAA Privacy Officer



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

REFERENCE GUIDE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call 1-877-322-8228, toll free.

Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329.
- Experian, P.O. Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, P.O. Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission (FTC) and/or the attorney general's office in your state. You can obtain information from these sources about steps you can take to avoid identity theft, as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Contact information for the FTC is as follows:

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

Fraud Alerts and Credit or Security Freezes

Fraud alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year.

You may have an extended alert placed on your credit report if you have already been a victim of identity theft, with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, free of charge, contact one of the nationwide credit bureaus. The credit bureau you contact must tell the other two and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an active-duty military fraud alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or security freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. Most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013, www.experian.com.
- TransUnion Security Freeze, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com.
- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com.

You'll need to supply your name, current and former addresses (for the past five years), date of birth, Social Security number, any applicable incident report or complaint with law enforcement or the Registry of Motor Vehicles, a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

After receiving your freeze request, each credit bureau will provide you with a unique personal identification number (PIN) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

State Specific Information

California residents may 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, (800) 952-5225.

Connecticut residents may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, (860) 808-5318 or at www.ct.gov/ag.

District of Columbia residents may obtain information from the District of Columbia's Attorney General's Office regarding steps to take to avoid identity theft. This office can be reached by visiting the website at <https://oag.dc.gov/>, calling (202) 727-3400, or visiting 400 6th Street NW Washington, D.C. 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky residents may contact the Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, (502) 696-5300 or at www.ag.ky.gov.

Maryland residents may learn more about preventing identity theft from the Maryland Office of the Attorney General by visiting its web site at <http://www.marylandattorneygeneral.gov/>, calling the Identity Theft Unit at (410) 567-6491 or requesting more information at: Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, (617) 727-8400 or at www.mass.gov/ago/contact-us.html. You are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above. For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York residents may contact the New York Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, (800) 771-7755 or <https://ag.ny.gov>.

North Carolina residents may learn more about preventing identity theft from the North Carolina Office of the Attorney General by visiting its website at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, calling (919) 716-6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at (401) 274-4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

South Carolina residents may access educational resources and the availability of consumer assistance from the South Carolina Department of Consumer Affairs. This office can be reached by visiting the website at <https://consumer.sc.gov/>, calling (803) 734-4200, or visiting 293 Greystone Boulevard Ste. 400, Columbia, SC 29210.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.