McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

November 29, 2021

VIA U.S. MAIL

North Dakota Attorney General
Office of Consumer Protection
600 E. Boulevard Ave., Dept. 125
Bismarck, ND 58505

Re: DNA Diagnostics Center, Inc. ("DDC") – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents DNA Diagnostics Center, Inc. ("DDC"). I am writing to provide notification of an incident at DDC that may affect the security of personal information of approximately three hundred fifty-seven (357) North Dakota residents. DDC's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, DDC does not waive any rights or defenses regarding the applicability of North Dakota law or personal jurisdiction.

DDC recently discovered potential unauthorized access to its network. Upon learning of the issue, DDC promptly opened an investigation. As part of its investigation, DDC has been working closely with external cybersecurity professionals. DDC has also coordinated closely with law enforcement following the discovery of this incident. After an extensive forensic investigation, DDC determined that the unauthorized individual(s) potentially removed certain files and folders from portions of DDC's database between May 24, 2021 and July 28, 2021. The impacted database was associated with a national genetic testing organization system that DDC has never used in its operations and has not been active since 2012. DDC determined on October 29, 2021, that the information that potentially may have been acquired included the residents' full names, Social Security numbers and in some cases credit or debit card information.

DDC is providing notification of this incident commencing on November 29, 2021, in substantially the same form as the documents attached hereto. DDC is advising affected individuals about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. Those individuals whose credit or debit card information was impacted are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. Individuals are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. Those individuals whose Social Security numbers may have been impacted are being offered complimentary credit monitoring through Experian.

213179

At DDC, protecting the privacy of personal information is a top priority. DDC is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. DDC continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

Encl.

DNA Diagnostics Center

Data Security Incident Information Center

We will keep this page updated with actions we are taking, including free credit monitoring and identity theft protection services for those whose personal information was potentially accessed.

What happened?

On August 6, 2021, DNA Diagnostics Center, Inc. (DDC) detected potential unauthorized access to its network, during which there was unauthorized access and acquisition of an archived database that contained personal information collected between 2004 and 2012. The impacted database was associated with a national genetic testing organization system that DDC acquired in 2012. This system has never been used in DDC's operations and has not been active since 2012.

Therefore, impacts from this incident are not associated with DDC. However, impacted individuals may have had their information, such as Social Security number or payment information, impacted as a result.

Upon learning of this issue, DDC proactively contained and secured the threat and executed a prompt and thorough investigation in consultation with third-party cybersecurity professionals. DDC has also coordinated closely with law enforcement following the discovery of this incident. Our investigation determined that the unauthorized individual(s) potentially removed certain files and folders from portions of our database between May 24, 2021 and July 28, 2021. DDC has been and remains fully operational, and the systems and databases that are actively used by DDC were not infiltrated.

The in-depth investigation concluded on October 29, 2021, and DDC has begun notifying individuals potentially affected by this incident.

How will you know if you were impacted?

If you know you have received a relationship test from DDC directly, this incident did not affect that test, as the information was acquired from an archived system that was never used by DDC.

Individuals whose personal information was potentially accessed are being notified in accordance with state regulations, and out of an abundance of caution to protect against identity fraud, DDC is providing a complimentary membership of Experian credit monitoring to eligible individuals.

If you received a relationship test as a part of court proceedings or independent, individual testing between 2004 and 2012 but have not received a mailed letter from DDC regarding this incident, please contact **1-855-604-1656** as you may be eligible for complimentary credit monitoring services through Experian.

What is DDC doing?

DDC has taken steps, in coordination with its third-party cybe
personal information and ensure its safekeeping. DDC is not

Hello! Do you want to know the status of your test?

use of the information.

Additionally, out of an abundance of caution, we are offering free credit monitoring for impacted individuals to protect against identity fraud – see below for more information. **Ensuring the safety and security of the personal information entrusted to us remains our primary responsibility, and we will continue to work with third-party experts to harden our cybersecurity defenses.**

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-855-604-1656 The response line is available Monday through Friday 9:00 AM to 9:00 PM, Eastern Standard Time, excluding U.S. Holidays

---

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION:

1. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	*Experian*	*TransUnion LLC*
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, PA 92834-6790
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	https://www.experian.com/fraud/center.html	https://www.transunion.com/frau alerts
(800) 525-6285	(888) 397-3742	(800) 680-7289

2. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	*Experian Security Freeze*	*TransUnion Security Freeze*
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-freeze/	http://experian.com/freeze	http://www.transunion.com/securityfreeze
(800) 349-9960	(888) 397-3742	(888) 909-8872

Hello! Do you want to know the status of your test?

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, https://oag.dc.gov/consumer-protection, Telephone: 1-202-727-3400.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319. www.iowaattorneygeneral.gov. Telephone: (515) 281-5164.

Hello! Do you want to know the status of your test?

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: 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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These 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. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

Hello! Do you want to know the status of your test?

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze — either completely, if you are shopping around, or specifically for a certain creditor — with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

Hello! Do you want to know the status of your test?

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were 234 Rhode Island residents impacted by this incident.

©2021 DNA Diagnostics Center. All Rights Reserved.

Hello! Do you want to know the status of your test?

DNA Diagnostics Center, Inc. Provides Notice of Data Security Incident

November 29, 2021 / Fairfield, OH – On August 6, 2021, DNA Diagnostics Center, Inc. (DDC) detected potential unauthorized access to its network, during which there was unauthorized access and acquisition of an archived database that contained personal information collected between 2004 and 2012. DDC has been and remains fully operational, and the systems and databases that are actively used by DDC were not infiltrated.

The impacted database was associated with a national genetic testing organization that DDC has never used in its operations and has not been active since 2012. DDC acquired certain assets from this national genetic testing organization in 2012 that included certain personal information, and therefore, impacts from this incident are not associated with DDC. However, impacted individuals may have had their information, such as Social Security numbers or payment information, impacted as a result.

Upon learning of this issue, DDC proactively contained and secured the threat and executed a prompt and thorough investigation in consultation with third-party cybersecurity professionals. DDC has also coordinated closely with law enforcement following the discovery of this incident. The investigation investigation determined that the unauthorized individual(s) potentially removed certain files and folders from portions of our database between May 24, 2021 and July 28, 2021.

The in-depth investigation concluded on October 29, 2021, and DDC has begun notifying individuals potentially affected by this incident.

DDC has taken steps, in coordination with its third-party cybersecurity experts, to regain possession of this personal information and ensure its safekeeping and is not aware of any reports of identity fraud or improper use of the information.

Individuals whose personal information was potentially accessed are being notified in accordance with state regulations, and out of an abundance of caution to protect against identity fraud, DDC is providing a complimentary membership of Experian credit monitoring to eligible individuals. If an individual was not notified of this incident directly via U.S. mail, but they think their information may have been involved because they received a relationship test as a part of court proceedings or independent, individual testing between 2004 and 2012, they should contact 1-855-604-1656 or visit https://dnacenter.com/data-security-incident-information-center/ for more information, as they may be eligible for complimentary credit monitoring services.

DDC encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors. Individuals may also review the guidance contained under "Steps Individuals Can Take to Protect Personal Information" on DDC's website, which can be accessed at https://dnacenter.com/data-security-incident-information-center/. The guidance provides additional information regarding fraud alerts and security freezes, as well as contact information for the nationwide consumer reporting agencies.

DDC will continue to work with third-party experts to harden our cybersecurity defenses, as ensuring the safety and security of the personal information entrusted to us remains our primary responsibility.

###