RECEIVED
ATTORNEY GENERAL OF OHIO

FEB 14 2023

CONSUMER PROTECTION SECTION
PUBLIC INSPECTION FILE

STATE OF OHIO
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION SECTION

IN THE MATTER OF)
DNA DIAGNOSTICS CENTER, INC.) DOCKET NO. 612037

ASSURANCE OF VOLUNTARY COMPLIANCE

Dave Yost, Attorney General of the State of Ohio ("Ohio Attorney General") and DNA Diagnostics Center, Inc. ("DDC"), collectively referred to as the "Parties", enter into an Assurance of Voluntary Compliance ("Assurance") pursuant to the Consumer Sales Practices Act, R.C. 1345.01 *et. seq.* ("CSPA").

This Assurance is entered into by the Attorneys General of Ohio and Pennsylvania (collectively, the "Attorneys General") and DDC to resolve the investigation by the Attorneys General into the data security incident announced by DDC on or about November 29, 2021 (the "Breach") that affected approximately 2.1 million United States residents.

1. ATTORNEYS GENERAL FINDINGS

1.1. DDC is a Delaware Foreign Limited Liability Company with its principal place of business located at One DDC Way, Fairfield, OH 45014.

1.2. Founded in 1995, DDC is one of the largest private DNA-testing companies, offering diagnostic and genetic tests to help answer relationship, fertility, and health and wellness questions. On its company's Linkedin page, it states, "DDC continues to expand its presence in the testing market through both its internal [Research and Development] efforts as well as acquisitions."[1]

1.3. The Attorneys General conducted an investigation under their states' respective consumer protection laws regarding the Breach involving the Social Security numbers of

[1] DDC Linkedin, https://www.linkedin.com/company/dna-diagnostics-center/ (last visited Sept. 9, 2022).

approximately 12,663 Pennsylvania residents and 33,282 Ohioans who were subject to genetic testing between 2004 and 2012 from a company that DDC acquired in 2012.

1.4. Specifically, the Breach involved databases that were not used for any business purpose, but were provided to DDC as part of a 2012 acquisition of Orchid Cellmark. In a December 19, 2011 press release, DDC's then President and CEO said of the Orchid Cellmark acquisition, "[o]ur acquisition of Orchid's government paternity business significantly expands the size and scope of DDC's portfolio, further solidifying our position as one of the largest DNA testing companies in the world."[2]

1.5. Although DDC expanded its portfolio after the Orchid Cellmark acquisition, DDC claims the Breach's impacted databases, containing sensitive personal information, were inadvertently transferred to DDC without its knowledge. Moreover, DDC asserts it was not aware that these legacy databases existed in its systems at the time of the Breach—more than nine years after the acquisition.

1.6. Prior to the Breach, DDC performed both an inventory assessment and a penetration test on its systems; however, the legacy databases that stored the sensitive personal information in plain text were not identified during these tests because the assessments only focused on active customer data.

1.7. As early as May 28, 2021, DDC's managed service provider began sending several automated alerts over a two-month period to DDC to notify the company that there was suspicious activity related to the Breach in DDC's network.

[2] https://www.prnewswire.com/news-releases/ddc-one-of-the-largest-dna-testing-companies-worldwide-further-expands-with-the-acquisition-of-orchid-cellmarks-government-paternity-business-135847093.html (last visited Sept. 9, 2022).

1.8. On August 6, 2021, the service provider notified DDC that there were indications of Cobalt Strike malware observed on DDC's network, which finally led DDC to activate its incident response plan.

1.9. A third-party investigation identified that the threat actor logged into a virtual private network ("VPN") on May 24, 2021 using a DDC user account. In addition, the threat actor harvested Active Directory credentials from a Domain Controller that provided password information for each account in the network. When the threat actor initially accessed the VPN, DDC had migrated to a different VPN and no users should have been using the VPN the threat actor used for remote access.

1.10. On June 16, 2021, the threat actor used a test account that had administrator privileges to create a persistence mechanism that executed Cobalt Strike throughout the environment.

1.11. Between July 7, 2021 and July 28, 2021, the threat actor accessed five servers and collectively backed up a total of 28 databases from the servers. In order to exfiltrate the data out of DDC's environment, the threat actor used a decommissioned server.

1.12. In September 2021, the threat actor contacted DDC and informed the company that the threat actor successfully exfiltrated sensitive personal information from DDC's network and demanded payment.

1.13. DDC provided payment to the hacker in exchange for the deletion of stolen data.

1.14. The Ohio Attorney General's investigation found that DDC engaged in deceptive or unfair business practices by making material misrepresentations in its customer-facing privacy policy concerning the safeguarding of its customers' personal information.

1.15. Specifically, DDC disseminated, or caused to be disseminated, the following statements on its website during the time of the Breach:

> We are committed to protecting the security of your information. We use a variety of reasonable security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. Access to your personal information is limited and we

take reasonable measures to ensure that your personal information is not accessible. Although DDC attempts to protect the personal information in its possession, no security system is perfect, and DDC cannot promise that your personal information will remain absolutely secure in all circumstances.[3]

1.16. The Ohio Attorney General alleges that DDC failed to employ reasonable measures to detect and prevent unauthorized access to its computer network. Therefore, the Ohio Attorney General alleges that DDC engaged in unfair and deceptive cybersecurity practices that taken together, unreasonably and unnecessarily exposed Ohio consumers' personal data to unauthorized access and theft.

1.17. The Ohio Attorney General alleges DDC's conduct constitutes unfair or deceptive acts or practices in the conduct of trade or commerce in violation of the CSPA, including without limitation, the following:

(i) Representing that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits that they do not have as prohibited by the CPSA, R.C. 1345.02(B)(1);

(ii) Representing that the subject of a consumer transaction is of a particular standard, quality, grade, style, prescription, or model if it is not, as prohibited by the CSPA, R.C. 1345.02(B)(2); and

(iii) Engaging in any other unfair or deceptive conduct in connection with a consumer transaction as prohibited by the CSPA, R.C. 1345.02.

1.18. Under R.C. 1345.06(F)(2) of the CSPA, this Assurance will not be considered an admission of wrongdoing for any purpose. For the purposes of this Assurance, DDC neither admits nor denies any of the Findings in this Section.

2. DEFINITIONS

2.1. "Compensating Controls" means alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer

[3] DDC Privacy, https://dnacenter.com/privacy-policy/ (last visited Sept. 9, 2022).

("CISO") or his or her designee to be impractical to implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must: (1) meet the intent and rigor of the original stated requirement; (2) provide a similar level of security as the original stated requirement; (3) be up-to-date with current industry accepted security protocols; and (4) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the Chief Information Security Officer or his or her designee agrees with both the risk analysis and the determination that the risk is acceptable.

2.2. "Consumer" means any Ohio consumer who provides Personal Information to DDC or to a company that DDC acquires through an acquisition.

2.3. "Effective Date" is the date on which both Parties have executed this Assurance.

2.4. "Personal Information" means information contained within DDC's network of Consumers that is "personal information" as defined under Security Breach Notification Act, R.C. 1349.19 (enacted March 30, 2007).

2.5. "Service Provider" means a third-party business entity that has expertise in providing comprehensive security analytics through detection and response to potential outside cybersecurity threats.

2.6. "State Consumer Protection Acts" means the Ohio Consumer Sales Practices Act, R.C. 1345.01 *et seq.*; Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1 *et seq.*

2.7. "State Personal Information Protections Acts" means the Ohio Security Breach Notification Act, R.C. 1349.19 *et seq.*; Pennsylvania Breach of Personal Information Notification Act, 73 P.S. §§ 2301 *et seq.*

2.8. "Vendor" means a third-party business entity that provides services to DDC and those services can potentially compromise the security of Personal Information.

3. APPLICATION

3.1. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance applies to DDC, its assigns, officers, and employees.

3.2. DDC must comply with the CSPA in connection with its collection, use, and maintenance of Personal Information, and must maintain reasonable security policies and procedures designed to safeguard Personal Information from unauthorized use or disclosure.

4. TERM

4.1. Unless otherwise specified herein, the requirements set forth below in Paragraphs 5.1-7.4 of this Assurance apply to DDC for a period of Five (5) years from the Effective Date.

5. INFORMATION SECURITY PROGRAM

5.1. DDC must further develop, implement, and maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that DDC collects, stores, transmits, and/or maintains, and that will, at a minimum include the requirements set forth in this Assurance to the extent appropriate based on DDC's assessment of relevant risks. A determination regarding the extent to which any such requirements defined in this Assurance are not appropriate must be based on a reasonable assessment of relevant risks and documented by DDC.

5.2. The Information Security Program must include the following components:

a. Documented methods and criteria for managing information security risks to Personal Information, including assessment, prioritization, reduction, and acceptance of risks. DDC's risk assessment methods and risk assessment criteria must conform to an information security risk assessment method that is provided by information security bodies (e.g., NIST Special Publications 800-30, The Sedona Conference Commentary on a Reasonable Security Test (February 2021), ISO 27005, Duty of Care Risk Analysis Standard ("DoCRA"), or Center for Internet Security Risk Assessment Method ("CIS RAM") Version 2.0) and must include the following:

i. The Information Security Program must design, implement, operate, test, and improve safeguards that reduce identified risks to a reasonable and appropriate level and achieve the control objectives listed below:

(a) The safeguards must not create a likelihood and impact of harm to Consumers or the public interest such that a remedy is needed.

(b) The safeguards may not require DDC to curtail its proper objectives (e.g., profit, growth, reputation, market competitiveness) or the utility of DDC's services to Consumers.

(c) The burden imposed on DDC by the safeguards must be proportionate to the risk the safeguards reduce to Consumers and the public interest.

b. DDC must conduct comprehensive risk assessments identifying where DDC stores Personal Information at least annually, and upon changes to its systems that may significantly increase risks to Consumers, DDC will assess the impact of the change. Comprehensive assessments must include intentional and unintentional foreseeable threats to Personal Information that could harm consumers. Risk assessments must be conducted by

parties that are competent to model threats that are relevant to DDC and who may capably estimate risks that are created by those threats.

c. Resources: DDC's allocation of risk-appropriate resources to protect Personal Information that may foreseeably harm Consumers and that sufficiently support DDC's claims about the effectiveness of its Information Security Program.

d. Designation of Responsible Parties: DDC's assignment of responsibility for operating the Information Security Program to personnel or Service Providers who have sufficient scope of authority and capability to effectively fulfill that role.

e. Information Security Program Assessment: At least annually, DDC must review the effectiveness of its Information Security Program and safeguards, and correction of vulnerabilities that may pose inappropriate risks. DDC must review the Information Security Program and controls with sufficient frequency and detail to provide timely and sufficient resources to address vulnerabilities and risks.

5.3. Such Information Security Program must be developed and implemented within One Hundred Eighty (180) days after the Effective Date of this Assurance. Failure to fully develop or implement such requirements within One Hundred Eighty (180) days after the Effective Date will not constitute a violation of this Assurance so long as DDC implements interim Compensating Controls to address the identified risks until such requirements are fully developed and implemented.

5.4. The DDC Information Security Program must be in writing and contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of DDC's operations; (ii) the nature and scope of DDC's activities; and (iii) the sensitivity of the Personal Information that DDC maintains.

5.5. DDC must retain an employee or Service Provider to be responsible for overseeing DDC's information security program with appropriate credentials, background and expertise in

information security who will be responsible for overseeing DDC's implementation and maintenance of the Information Security Program.

5.6. DDC's Information Security Program must include security awareness training designed to communicate DDC's commitment to full compliance with the Information Security Program and to ensure that all personnel with key responsibilities for implementation and oversight of the Information Security Program, including the person responsible for overseeing the implementation and maintenance of the program (e.g., CISO), have sufficient knowledge of the requirements of this Assurance, and the specific knowledge, skills, and abilities to perform their functions in compliance with the Information Security Program. DDC's training must ensure that system, database, network administrators, and persons with privileged access to Personal Information are fully informed of the requirements of the Information Security Program relevant to their functions, which may include password policies, secure data handling, secure storage, transmission and disposal of Personal Information, and best practices to prevent attackers from obtaining credentials and other sensitive data through malicious downloads and other threats identified by DDC. DDC must also develop accountability metrics to measure each participant's compliance with training requirements. Within Ninety (90) days of the Effective Date, DDC must provide training required by this Assurance, and thereafter will provide it to relevant personnel on at least an annual basis.

6. INFORMATION SECURITY SAFEGUARDS

6.1. When acquiring technical assets (e.g., systems, applications, or devices) containing Personal Information from other organizations, such as by acquisition of a business, DDC must assess risks associated with those assets and apply reasonable and appropriate security safeguards as defined in 5.2.a.i above. Notwithstanding risk evaluation, DDC must remove Personal Information from those assets where it serves no legitimate business purpose or utility to Consumers.

6.2. DDC must evaluate risks that could impact Personal Information posed by Vendors. DDC may achieve this objective through risk evaluating and auditing third parties to determine whether they meet DDC's acceptable risk definition, or may rely on independent third party auditors or certifications (e.g., ISO 27001 Certifications) that verify the third party's risk management program meets DDC's requirements.

6.3. As part of the Information Security Program, DDC must implement reasonable security for Personal Information by fulfilling control objectives that would have prevented or detected the Breach:

a. Personal Information must be transmitted and stored so that it is accessible only to people and systems that need the information for a legitimate business purpose. DDC may achieve this objective by encrypting, tokenizing, or de-identifying Personal Information.

b. DDC must maintain a current data/asset inventory of its entire network.

c. DDC must disable and/or remove any assets identified in its asset inventory that are not necessary for any legitimate business purpose performed on the DDC network.

d. DDC must implement its incident response plan that requires its employees to respond to any alerts that generated from its security monitoring systems and document the actions taken in response to the alerts.

e. DDC must reasonably know the location and disposition of Personal Information. DDC may achieve this objective through the use of process diagrams and procedures, information classification procedures, data scanning and inventory systems, asset scanning or management systems, or other means.

f. Personal Information that may harm the public if compromised must be reasonably separated from people and systems that can foreseeably compromise them, and must be reasonably separated from people, systems, and networks that are configured to be

less secure than DDC's risk acceptance criteria. DDC may achieve this objective by using network segmentation and other technical, physical, automated, or logical means.

g. DDC must detect, investigate, contain, respond to, eradicate, and recover from security incidents within reasonable time periods. DDC will achieve this objective using a documented incident response plan, trained personnel, experts, and tools that sufficiently address the risks of harm cause by security incidents. The plan will include the responsible determination of whether and how to disclose the incident to potentially affected parties and authorities.

h. DDC must ensure that people and systems that use credentials are who they purport to be by using technical, physical, or procedural mechanisms that are commensurate with the risk posed by abusing access to Personal Information. DDC may achieve this objective by providing multi-factor authentication, one-time passcodes, location-specific requirements, or other control enhancements.

i. DDC must implement and maintain logging and log monitoring policies and procedures designed to collect, manage, and analyze security logs and monitor where DDC stores Personal Information to detect, understand, or recover from an attack. DDC may achieve this objective by using a central log management system and log harvesting, parsing, alerting to be notified of anomalies or suspicious activity.

j. DDC must store event logs and security logs for a period of time that is sufficient to detect, respond to, and investigate security incidents. DDC may achieve this objective by estimating their time-to-respond during tests of their incident response plan and setting log repository retention periods accordingly.

k. DDC must maintain, keep updated, and support the software on its network, taking into consideration the impact a software update will have on data security in the

context of its network and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. For any software that will no longer be supported by its manufacturer or a third party, DDC must commence the evaluation and planning to replace the software or to maintain the software with appropriate Compensating Controls to address the identified risks within a reasonable time period from the date the manufacturer or third party announces that it is no longer supporting the software.

l. DDC must detect and respond to suspicious network activity within its network within reasonable means. DDC may achieve this objective by using log correlation and alerting, file integrity monitoring, data integrity monitoring, SIEM systems, intrusion detection and prevention systems (IDS/IPS), threat management systems, and other methods and tools.

7. SETTLEMENT COMPLIANCE ASSESSMENT

7.1. DDC must obtain an information security compliance assessment and report from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), within one (1) year after the Effective Date of this Assurance. The Third-Party Assessor's report must:

A. Set forth the specific administrative, technical, and physical safeguards maintained by DDC;

B. Explain the extent to which such safeguards are appropriate in light of DDC's size and complexity, the nature and scope of DDC's activities, and the Personal Information that is handled by DDC;

C. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program.

7.2. DDC's Third-Party Assessor must (a) be a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and (b) have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

7.3. Within ninety (90) days of completion of the Third-Party Assessor's report, DDC must notify the Ohio Attorney General of the completion of the report. If the Ohio Attorney General seeks a copy of the Third-Party Assessor's report, the Ohio Attorney General will issue a subpoena pursuant to R.C. 1345.06(B) to direct DDC to produce and deliver or cause to deliver a copy of the report to the Ohio Attorney General.

7.4. The identification of any deficiencies or recommendations for correction in the Third Party Assessor's report will not constitute a violation of this Assurance unless such deficiencies otherwise amount to a violation of the other obligations set forth in this Assurance.

8. PAYMENT TO STATES

8.1. DDC will pay $400,000.00 (Four Hundred Thousand dollars and 00/100) to the Attorneys General. Payment must be made no later than thirty (30) days after the Effective Date of this Assurance and receipt of such payment instructions by DDC from the Attorneys General. The Ohio Attorney General's portion of the payment is $200,000.00 (Two Hundred Thousand Dollars and 00/00).

8.2. The payments received by the Attorneys General may be used for purposes that may include, but are not limited to, attorneys' fees, and other costs of investigation and litigation, or may be placed in, or applied to, any consumer protection enforcement fund, including future consumer protection or privacy enforcement, consumer education or redress, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, and/or for other uses permitted by state law.

9. RELEASE

9.1. Following full payment of the amounts due under this Assurance, the Attorneys General will hereby release and discharge DDC, its assigns, officers, and employees from all civil claims that the Attorneys General could have brought under the State Consumer Protection Acts, the State Personal Information Protection Acts, state security breach notification acts, or common law claims concerning unfair, deceptive or fraudulent trade practices based on DDC's alleged conduct related to the Breach. Nothing contained in this paragraph will be construed to limit the ability of the Attorneys General to enforce the obligations that DDC has under this Assurance, identified in Paragraphs 3.2, 5.1-7.4. Further, nothing in this Assurance will be construed to create, affect, limit, alter, or assist any private right of action, including without limitation any private right of action that a consumer or other third-party may hold against DDC. This Assurance may be enforced only by the Parties hereto.

10. GENERAL PROVISIONS

10.1. This Assurance shall be governed by the laws of the State of Ohio.

10.2. This Assurance sets forth the entire agreement between the Ohio Attorney General and DDC and supersedes any and all prior agreements or understandings, whether written or oral, between the parties and/or their respective counsel regarding the subject matter hereof. This Assurance may be amended by written agreement of the Parties, subject to any further requirements under state law.

10.3. The Parties hereto acknowledge that no other promises, representations, or agreements of any nature have been made or entered into by the Parties. The Parties further acknowledge that this Assurance constitutes a single and entire agreement that is not severable or divisible, except that if any provision herein is found to be legally insufficient or unenforceable, the remaining provisions shall continue in full force and effect.

10.4. This Assurance constitutes a public record and shall be placed in the Public Inspection File pursuant to R.C. 1345.05(A)(3).

10.5. The Parties understand and agree that this Assurance will not be construed as an approval or a sanction by the Ohio Attorney General of DDC's business practices, nor will DDC represent that this Assurance constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Ohio Attorney General to take any action in response to any information submitted pursuant to this Assurance will not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor will it preclude action thereon at a later date.

10.6. Nothing in this Assurance will be construed as relieving DDC of the obligation to comply with all state and federal laws, regulations, and rules, nor will any of the provisions of this Assurance be deemed to authorize or require DDC to engage in any acts or practices prohibited by such laws, regulations, and rules.

10.7. DDC must deliver a copy of this Assurance to, or otherwise fully apprise, each of its current officers of the rank of executive vice president or above, the executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each member of its Board of Directors within ninety (90) days of the Effective Date. DDC must deliver a copy of this Assurance to, or otherwise fully apprise, any new officers of the rank of executive vice president or above, new executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each new member of its Board of Directors, within thirty (30) days from which such person assumes his/her position with DDC.

10.8. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which will constitute an original counterpart thereof and all of which together will constitute one and the same document. One or more counterparts of this

Assurance may be delivered by facsimile or electronic transmission with the intent that it or they will constitute an original counterpart thereof.

10.9. If any clause, provision, or section of this Assurance is held to be illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability will not affect any other clause, provision, or section of this Assurance, which will be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

10.10. Whenever DDC provides notice to the Ohio Attorney General under this Assurance, that requirement will be satisfied by sending notice to Assistant Attorney General Christopher Ramdeen, 30 E. Broad St., 14th Floor, Columbus, Ohio 43215. Any notices sent to DDC pursuant to this Assurance will be sent to the following addresses: DNA Diagnostics Center, Inc., One DDC Way, Fairfield, OH, 45014, Attn: Jason Judd and McDonald Hopkins, LLC, 39533 Woodward Avenue, Suite 318, Bloomfield Hills, MI 48304, Attn: Dominic Paluzzi. Any Party may update its address by sending written notice to the other Party. All notices under this Assurance will be provided via overnight mail. DDC certifies that Jason Judd is authorized by DDC to enter into this Assurance on behalf of DDC and that his/her signature on this document binds DDC to all terms herein.

NOW THEREFORE, DDC agrees by signing this Assurance, DDC must abide by each and every one of the aforementioned terms of this Assurance and that the Ohio Attorney General may enforce this Assurance pursuant to the CSPA, R.C. 1345.06(F)(2) by petitioning any Court of competent jurisdiction, to order any equitable or other relief which may be deemed necessary and appropriate as provided herein and by law.

STATE OF OHIO
OFFICE OF ATTORNEY GENERAL

DAVE YOST
OHIO ATTORNEY GENERAL

Date: 2-14-23 By: _____

CHRISTOPHER RAMDEEN
Associate Assistant Attorney General
30 East Broad Street, 14th Floor
Columbus, Ohio 43215-3400
Phone: (614) 995-1577
Christopher.Ramdeen@OhioAttorneyGeneral.gov

DNA DIAGNOSTICS CENTER, INC.

Date: 2/13/2023 By: _____

Jason Judd
President
One DDC Way
Fairfield, OH, 45014

Counsel to DNA Diagnostics Center, Inc.

Date: 2/13/2023 By: _____

Dominic A. Paluzzi (P71666)
Kate Jarrett (P84576)
McDonald Hopkins LLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304