

# **EXHIBIT B**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

---

GENOMIC PREDICTION, INC.,

Plaintiff,

Case No.

vs.

**DECLARATION OF KIM  
MILLER**

NATHAN TREFF, TALIA METZGAR and  
NUCLEUS GENOMICS, INC.,

*Filed Electronically*

---

Defendants.

**DECLARATION OF KIM MILLER**

Kim Miller, of full age, hereby certifies:

1. I am the Solutions Architect and Director of Customer Success for Genomic Prediction, Inc. (“GP”). I make this Declaration based upon personal knowledge and my review of the business records maintained by GP.

**GP Protects the Confidentiality of its Trade Secrets and Confidential Information**

2. GP expends significant time, resources and money in protecting from disclosure the confidentiality of its trade secrets and all of its confidential and proprietary information including electronically stored information.

3. In addition, because GP deals with sensitive personal and medical information and data belonging to patients and customers, GP uses the utmost care in protecting that information and data from disclosure

4. Access to GP’s systems, including email and shared drives, is password protected, subject to multi-factor authentication (“MFA”), and controlled by a central administrator.

5. GP enforces strong password policies with specific character requirements.
6. GP also remotely manages all its electronic devices, such that if a laptop or tablet containing GP information is lost or stolen, GP can wipe that device clean of the information remotely.
7. GP also instructs all employees to lock their electronic devices when they are unattended to ensure those devices are always password protected.
8. GP employees who are trying to access GP's systems from outside of a GP office must use a virtual private network ("VPN") that is operated by GP and kept secure. Logging in using MFA is required to access the VPN. Accessing VPN also requires passing through SonicWall Firewall.
9. Most of GP's confidential information is kept on network attached storage ("NAS") that cannot be accessed from outside of the lab without being on VPN and getting through the SonicWall Firewall.
10. GP uses one physical server to store information and that server is kept behind lock and key. Currently, I am the only GP employee with a key.
11. GP also uses Google Workspace, which cannot be accessed without using MFA.
12. GP also has a set of "Controlled Documents" in Google Workspace.
13. These Controlled Documents are proprietary and confidential forms and workflows that only a small number of employees can access, edit, or download.
14. Employees at GP have differing levels of access to GP's systems and information based on their position and department.
15. Access profiles are set for each employee when they are hired and are designed to give each individual employee access to only what is necessary for them to perform their duties.

16. In particular, data from GP's wet lab, data from the clinical portal, and other data related to GP's trade secret processes for interpreting DNA are heavily restricted.

17. During the onboarding process and annually, employees receive training about cybersecurity and the protection of confidential information, including as it relates to compliance with the Health Information Portability and Accountability Act ("HIPAA").

18. Employees also receive a long list of expectations regarding how to protect confidential and trade secret information during onboarding in both the Employee Handbook and during the training process

19. The GP Employee Handbook contains policies requiring GP employees to maintain the confidentiality of GP's proprietary information.

20. Upon termination, an employee's access to any GP systems and files is withdrawn.

21. Employees are required to return all devices, documents, and information in their possession on their last day of work for GP.

22. The physical lab space where GP performs its work is also locked. A strictly limited number of people have keys to the lab. After Treff's departure, the locks were changed.

#### **Nathan Treff's Deletion of Data**

23. On August 12, 2025, I was asked to go to the lab to change the locks to the lab.

24. While I was there, I saw that defendant Nathan Treff ("Treff") had left his GP laptop in the lab.

25. I confirmed it was his laptop by looking at the serial number and asset tag on the laptop.

26. When I opened the laptop, a “Hello” screen appeared and there were no existing user profiles on the laptop. That indicated to me that the laptop had been reset to factory settings, which would have erased all data on the laptop.

27. In addition, there are eight Ring cameras placed throughout the lab.

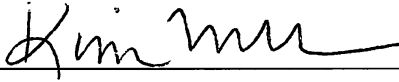
28. Because of Treff’s role in the lab, he set up the Ring camera account using his GP email address, and only he had access to the Ring footage during his employment.

29. At 4:50pm on August 12, 2025, the day of his departure from GP, Treff canceled his Ring subscription.

30. GP had no other way to access the Ring footage.

I declare under penalties of perjury under the laws of the United States and New Jersey  
that the foregoing is true and correct.

Dated: October 22, 2025

A handwritten signature in black ink, appearing to read "Kim Miller", is written over a horizontal line.

Kim Miller