**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF RHODE ISLAND**

| | | |
|---|---|---|
| UNITED STATES OF AMERICA ex rel. [UNDER SEAL] | ) | |
| Plaintiff-Relator | ) | **Civil Action No. _____** |
| v. | ) | |
| [UNDER SEAL] | ) | **FILED IN CAMERA AND UNDER SEAL PURSUANT TO 31 U.S.C. § 3730(b)(2)** |
| Defendant | ) | **Jury Trial Requested** |

# COMPLAINT

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF RHODE ISLAND**

| | | |
|---|---|---|
| UNITED STATES OF AMERICA ex rel. ERICA A. LENORE | ) | |
| Plaintiff-Relator | ) | **Civil Action No. _____** |
| v. | ) | |
| ILLUMINA, INC. | ) | **FILED IN CAMERA AND UNDER SEAL PURSUANT TO 31 U.S.C. § 3730(b)(2)** |
| Defendant | ) | **Jury Trial Requested** |

# COMPLAINT

# Table of Contents

This is a False Claims Act *qui tam* action by Relator to recover treble damages and civil penalties arising from the actions of Illumina, Inc. ("Illumina").

## I. STATEMENT OF THE CASE

1. Illumina is an American publicly traded biotechnology company with over 10,000 employees and develops and manufactures products to perform newly developed genetic testing. Illumina controls over 80 percent of the global genetic market, receiving some money from private equity firms.

2. The Government also directly funds Illumina through grants, contracts, and awards from dozens of federal agencies. Illumina is indirectly funded by the Government through NIH grants and awards to research institutions and the VA, which either seek to purchase Illumina products or are already using Illumina products to perform genetic sequencing analysis. Private organizations like laboratories purchase and use Illumina products to diagnose and treat Medicare patients, which is another way in which Illumina is indirectly funded by the Government. Illumina is also the sole authorized servicer for its own products; thus, all these purchasers are dependent on Illumina for servicing contracts for the operating life of the products.

3. Illumina has received at least hundreds of millions of dollars in Medicare reimbursement through these various sources.

4. Confidential patient data is housed on all Illumina products including HIPAA-protected data of Medicare beneficiaries such as their genetic test results. The Government trusts Illumina to have cybersecurity protections in place to protect this confidential data.

5. The FDA regulates medical products including Illumina products through Quality System regulation ("QSR"). Three of the major components outlined in the QSR and applicable to Illumina products are design control, corrective and preventative action, and management. 21 CFR § 820 *et seq*.

6. However, Illumina has completely disregarded these requirements in its race to develop and maintain control of the global genetic testing market. Despite known widespread cybersecurity failures in its products at launch and its on-market products, Illumina continues to push out new products with cybersecurity vulnerabilities and has failed to mitigate or correct problems in its on-market products. Thus, the Government has not gotten what it paid for.

7. Illumina's knowing and continuing cybersecurity failures include:

- improper granting of elevated privileges to everyday users by default (analogous to having super admin rights of a database);
- failures to protect the credentials of everyday users by allowing their account user names and passwords to be generally accessible through hard coding of its software products (obviating the need

for authentication and encryption before accessing or manipulating data); and

- failures to mitigate or correct the risk of insider threats.

8. Because of these undisclosed cybersecurity defects, Illumina has knowingly allowed thousands of Illumina insiders and everyday users of its products the ability to access and manipulate HIPAA-protected patient genomic data including test results and to do so without detection.

9. Illumina's knowledge of material cybersecurity failures long pre-dated the launch of its products. Any mitigation has been involuntary and only in reaction to complaints from third parties that malicious actors had exploited vulnerabilities in its products. In its first product recall, in August 2022, Illumina disclosed to the Government a known cybersecurity vulnerability in its Local Run Manager software—nearly one year after a third party notified Illumina of the vulnerability. Illumina classified the vulnerability as "critically severe." The recall disclosed for the first time that Illumina improperly allowed everyday users elevated privileges and failed to implement basic cybersecurity safeguards such as authentication and encryption.

10. In April 2023, Illumina disclosed to the Government a cybersecurity vulnerability in another of its products called Universal Copy Service, describing it in limited terms as "an unnecessary privileges" vulnerability. Both recalls were the

result of the same vulnerabilities, which remained and continue to remain outstanding. And both recalls were half-truths because at the time of the recalls, Illumina was aware that the same vulnerabilities existed in other Illumina products—both on-market products and those about to be launched—but knowingly failed to recall those products as well. It was also aware of the existence of other undisclosed cybersecurity vulnerabilities in its products.

11. Illumina has knowingly continued to allow thousands of everyday users to have unauthorized access to its products, networks, and credentials (such as user names and passwords), and to manipulate, supplement, and delete confidential patient data; change product configurations and settings; install unauthorized applications; grant third-parties access to the system; disable firewalls and other operating-system-level protections; enable external attacks on the system; and alter patient genomic test results.

12. Illumina products currently on the market continue to contain material cybersecurity vulnerabilities, which threaten the integrity of the testing data produced by the products and compromise patient confidentiality.

13. As such, Illumina continues to make materially false certifications to the Government about the cybersecurity protections of its products. Through its fraudulent course of conduct, Illumina knowingly submitted or caused to be submitted false or fraudulent claims under Government contracts, grants, and

programs and Medicare claims, in violation of the False Claims Act, and the Government paid those claims.

14. In addition to taxpayers, victims of this fraud also include patients who have no idea that their genomic data is available on the marketplace and able to be manipulated inadvertently or by malicious actors.

15. This case is precisely the type of fraud scheme that the U.S. Department of Justice seeks to remedy under the False Claims Act through its Civil Cyber-Fraud Initiative to "hold accountable entities or individuals that put U.S. information or systems at risk by

- knowingly providing deficient cybersecurity products or services
- knowingly misrepresenting their cybersecurity practices or protocols, or
- knowingly violating obligations to monitor and report cybersecurity incidents and breaches."

16. "[P]rotecting against malicious cyber campaigns is a matter of national concern and a top priority for the [current] Administration." Thus, "[w]hen companies that do business with the government knowingly make misrepresentations about their own cybersecurity practices, or when they fail to abide by cybersecurity requirements in their contracts, grants or licenses, the government does not get what it bargained for." And "when false assurances are

made to the government, sensitive government information and Systems may be put at risk without the government even knowing it." Press Release, Office of Public Affairs, U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative; Remarks of Brian Boynton, Acting Assistant Attorney General, Civil Division, U.S. Department of Justice (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and

17. The Deputy Attorney General further directed comments at whistleblowers: "to those who witness irresponsibility that exposes the government to cyber breaches, our message is this: if you see something, say something." But for Relator, the Government would not be on notice of the allegations in this Complaint. Remarks of Lisa O. Monaco, Deputy Attorney General, U.S. Department of Justice (Oct. 20, 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr

18. Use of the False Claims Act as an enforcement tool will hold Illumina accountable for its knowing and material cybersecurity failures, deter future cyber misconduct by Illumina and other companies that do business with the

Government, and protect sensitive Government and patient data from exposure in the event of future attacks on Illumina products.

## II. LEGAL FRAMEWORK

### A. Parties

19. Relator alleges, based upon personal knowledge, relevant documents, and on information and belief, the facts set forth in this Complaint. Relator has first-hand knowledge of Defendant's pattern and practice alleged.

20. Relator has standing to bring this action under 31 U.S.C. § 3730(b)(1). Relator's allegations have not been publicly disclosed as that term is defined under 31 U.S.C. § 3730(e)(4)(A). Even if Relator's allegations had been publicly disclosed, Relator is the original source of the allegations in this Complaint under 31 U.S.C. § 3730(e)(4)(B).

21. Relator has complied with all procedural requirements of the laws under which this Complaint is brought.

22. Relator was retaliated against and terminated because of lawful acts by Relator to stop one or more violations of the False Claim Act and lawful acts by Relator in furtherance of an action under 31 U.S.C. § 3730.

23. Defendant Illumina Inc. ("Illumina") is an American, publicly traded biotechnology company founded in 1998 with approximately 10,000 employees. It is incorporated in Delaware and headquartered in San Diego, California. The

Rhode Island – IDeA Network of Biomedical Research Excellence (RI-INBRE), funded in part by the NIH, relies on Illumina's MiSeq product for biomedical research performed by hundreds of researchers and thousands of students affiliated with the University of Rhode Island.

24. With an annual revenue of $4.58 billion, Illumina represents on its website that its "customers include a broad range of academic, government, pharmaceutical, biotechnology, and other leading institutions around the globe."

25. Illumina dominates the genetic testing market – also known as next generation sequencing or NGS – with an 80 percent share. In 2022, "the NGS market is expected to hit nearly $12 billion, and it's forecast to increase to $22.7 billion by 2025." It has received tens of millions of dollars in private equity and venture funding from investors, including the Tisch Family Fund, Lombard Odier & Cie, State Farm Automobile Insurance Company, Chase Capital Partners, PE Corporation, the Dow Chemical Company, Chevron Technology Ventures, Venrock Associates, ARCH Venture Partners, CW Group, and Tredegar Investments. Illumina also partners with private equity and venture firms to develop new technologies. In 2015, private equity firm Warburg Pincus LLC and venture capital firm Sutter Hill Ventures invested $100 million in Illumina to support the company's efforts to develop a new consumer-facing human genome platform. Other Illumina investors include activist investor Carl Icahn who owns a

1.4 percent stake in the company.

### B. Jurisdiction and Venue

26. This Court has jurisdiction over the subject matter and all parties to this action pursuant to 28 U.S.C. §§ 1331, 1345, and 1367(a) because this is a civil action by Relator on behalf of the United States, the real party in interest, arising under the FCA qui tam provisions, and all claims in the action form part of the same case or controversy.

27. The Court has personal jurisdiction over Defendant pursuant to 31 U.S.C. § 3732(a) because Defendant resides, transacts business, or committed an act proscribed by the FCA within this District.

28. Venue is proper in this judicial district and its division, pursuant to 31 U.S.C. § 3732(a), because Defendant transacts business in this District, or because an act, proscribed by 31 U.S.C. § 3729, occurred in this District.

### C. Time Period

29. Defendant's conduct alleged in this Complaint began at least as early as 2016 and is continuing. All the claims in this matter are timely under 31 U.S.C. §3731(b).

**D. The False Claims Act**

30. The False Claims Act ("FCA") provides, in part, that any person who knowingly presents, or causes to be presented, a false claim for payment or approval; or knowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim; or knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government, is liable to the United States for penalties and treble damages. 31 U.S.C. §§ 3729(a)(1)(A), (B), (G). The FCA defines the term "obligation" to include an established duty arising from a grantor-grantee relationship. 31 U.S.C. § 3729(b)(3).

31. Knowingly means that the person: (1) had actual knowledge of the information; (2) acted in deliberate ignorance of the truth or falsity of the information; or (3) acted in reckless disregard of the truth or falsity of the information. The person need not have acted with specific intent to defraud the United States to be liable under the FCA. 31 U.S.C. § 3729(b)(1).

32. A "claim" under the False Claims Act includes any request or demand, whether under a contract or otherwise, for money or property that is

presented to an officer, employee, or agent of the United States." 31 U.S.C. § 3729(b)(2)(A)(i).

33. The term "material" means having a natural tendency to influence, or be capable of influencing, the payment or receipt of money. 31 U.S.C. § 3729(b)(4).

34. Violations of the FCA subject the defendant to mandatory civil penalties per FCA violation, plus three times the amount of damages that the Government sustains as a result of the defendant's actions. 31 U.S.C. § 3729(a).

35. A person known as a relator may bring a civil action for a violation of 31 U.S.C. § 3729 for the person and for the United States Government. The action shall be brought in the name of the Government. 31 U.S.C. § 3730(b)(1). If the Government elects not to proceed with the action, the person who initiated the action shall have the right to conduct the action. 31 U.S.C. § 3730(c)(3). If the Government does not proceed with an action under this section, the person bringing the action or settling the claim shall receive an amount which the court decides is reasonable for collecting the civil penalty and damages. The amount shall be not less than 25 percent and not more than 30 percent of the proceeds of the action or settlement and shall be paid out of such proceeds. Such person shall also receive an amount for reasonable expenses which the court finds to have been

necessarily incurred, plus reasonable attorneys' fees and costs. All such expenses, fees, and costs shall be awarded against the defendant. 31 U.S.C. § 3730(d)(2).

36. An employee shall be entitled to all relief necessary to make that employee whole, if that employee is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment because of lawful acts done by the employee in furtherance of an action under this section or other efforts to stop 1 or more violations of the FCA. 31 U.S.C. § 3730(h)(1). Relief shall include reinstatement with the same seniority status that employee would have had but for the discrimination, 2 times the amount of back pay, interest on the back pay, and compensation for any special damages sustained as a result of the discrimination, including litigation costs and reasonable attorneys' fees. 31 U.S.C. § 3730(h)(2).

## III. THE REGULATORY FRAMEWORK

### A. FDA Requirements for Medical Products

37. The Food and Drug Administration ("FDA") regulates medical products through the Quality System regulation ("QSR"). 21 C.F.R. § 820. The QSR provides a framework of the minimum requirements that a manufacturer must comply with to produce a safe and effective quality system. In 1996, when the FDA revised its manufacturing requirements for medical products and incorporated them into the QSR, the FDA explained that:

> Because this regulation must apply to so many different types of devices, the regulation does not prescribe in detail how a manufacturer must produce a specific device. Rather, the regulation provides the framework that all manufacturers must follow by requiring that manufacturers develop and follow procedures and fill in the details that are appropriate to a given device according to the current state-of-the-art manufacturing for that specific device.

38. Three of the major subsystems outlined in the QSR are design controls; corrective and preventative action; and management. 21 CFR § 820 *et seq*.

39. Design controls is one of the major QSR subsystems. For all classes of medical devices and products automated with software, a manufacturer is required to establish and maintain procedures to control the design of the device to ensure that specified design requirements are met. As part of the design controls requirements, a manufacturer must "establish and maintain procedures for validating the device design" that "include software validation and risk analysis, where appropriate." Because design controls are important to ensure medical device and product cybersecurity, the "FDA recommends that device manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the QSR." Cybersecurity risk management programs "should address the identification of security risks, the design requirements for how the risks will be controlled, and

the evidence that the controls function as designed and are effective in their environment of use for ensuring adequate security." In particular, the FDA recommends that a company undertake system requirements, threat mitigation, vulnerability testing, and penetration testing (a form of software security validation), and include resulting security testing documentation and any associated reports or assessments in its premarket submission. 21 CFR § 820.30 *et seq*., (a), (g)

40. Corrective and preventive action ("CAPA") is another of the major QSR subsystems. The CAPA subsystem requires manufacturers to "identify and investigate product and quality problems" and "take appropriate and effective corrective and/or preventive action to prevent their recurrence." "Verifying or validating corrective and preventive actions, communicating corrective and preventive action activities to responsible people, providing relevant information for management review, and documenting these activities are essential in dealing effectively with product and quality problems, preventing their recurrence, and preventing or minimizing device failures." The FDA has reinforced to medical device manufacturers that implementation of comprehensive cybersecurity risk management programs, and documentation of such, are material to compliance with CAPA requirements. CAPA also requires manufacturers to document all CAPA-required activities and the results of

those activities. 21 CFR § 820.100 (a), (b).

41. Management is another of the QSR's major subsystems. 21 CFR §§ 820.20, 820.22, 820.25. The QSR defines "management with executive responsibility" ("management") as "those senior employees of a manufacturer who have the authority to establish or make changes to the manufacturer's quality policy and quality system." 21 CFR § 820.3(n). "Quality policy" is defined as "the overall intentions and direction of an organization with respect to quality, as established by management with executive responsibility." 21 CFR § 820.3(u). "Quality system" is defined as "the organizational structure, responsibilities, procedures, processes, and resources for implementing quality management." 21 CFR § 820.3(v). Under the QSR, management is tasked with "establish[ing] its policy and objectives for, and commitment to, quality." 21 CFR § 820.20(a). Management must also "ensure that the quality policy is understood, implemented, and maintained at all levels of the organization." 21 CFR § 820.20(a). Management must also "review the suitability and effectiveness of the quality system at defined intervals and with sufficient frequency according to established procedures to ensure that the quality system satisfies the requirements of this part and the manufacturer's established quality policy and objective." 21 CFR § 820.20(c). "The dates and results of quality system reviews shall be documented." 21 CFR § 820.20(c).

Management may delegate the performance of quality activities to others, but management may not delegate the responsibility. That is, management is ultimately responsible for ensuring that the quality system is being implemented and that it is effective.

42. The QSR also contains regulations governing nonconforming products. Manufacturers are required to "establish and maintain procedures to control product that does not conform to specified requirements." These procedures should "address the identification, documentation, evaluation, segregation, and disposition of nonconforming product." As part of a manufacturer's evaluation of the nonconforming product, the manufacturer is expected to determine the need for an investigation. The manufacturer is expected to document the evaluation and any investigation. 21 C.F.R. § 820.90(a).

43. Product manufacturers who fail to comply with these FDA cybersecurity and conforming product regulations have recalled their products from the market due to the significant vulnerabilities. FDA recognizes that "[f]ailure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or network to security threats," and could "result in patient illness, injury or death." The FDA repeatedly reminded the industry that:

> Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity. An effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to obsolescence It is recommended that manufacturers apply the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond and Recover)

### B. Government Funding for Illumina Products

44. Illumina has received federal dollars through grants, contracts, and awards from dozens of federal agencies (direct funding). Illumina also indirectly receives federal dollars, for example, through NIH grants and awards to research institutions and the VA, which either seek to purchase Illumina products or are already using Illumina products to perform sequencing analysis (indirect funding). Further, private organizations purchase and use Illumina products to diagnose and treat Medicare patients; thus, Illumina has caused third-party entities that used its products to submit claims to Medicare.

45. Since 2001, Illumina has received at least $530 million in direct funding from federal agencies, with at least $43 million in 2022 alone.

46. Illumina is also the sole authorized servicer for its products. In practice, this means that once a federal agency buys an Illumina product, the agency is tied to Illumina for servicing contracts for the operating life of the

product. Since 2001, federal agencies have paid Illumina over tens of millions of dollars for maintenance services alone.

47. As examples of indirect funding, in 2021, NIH funded the University of Texas to purchase an Illumina NovaSeq 6000 Sequencing System, for use by the University's Greehey Children's Cancer Research Institute; in 2019, NIH funded the Northport VA Medical Center to purchase an Illumina NextSeq 550 Sequencing System, for use to evaluate cell-specific variation in diseases related to the center's mission.

48. As examples of private organizations that purchase and use Illumina products to diagnose and treat Medicare patients, Foundation Medicine, Inc., a molecular information company that offers genomic profiling assays to identify tumors and match patients with treatments, performs tests on Medicare patients. On information and belief, between 2018 and 2020, it received hundreds of millions of dollars in Medicare reimbursement for tests performed with Illumina products. On information and belief, between 2018 and 2020, for tests performed using Illumina products, Myriad Genetic Laboratories, Inc., a genetic and precision medicine company that offers genetic tests to identify cancer and other diseases with genetic markers, received at least over $160 million in Medicare reimbursements; and Guardant Health, a precision oncology company that tests patients for early- to late-stage cancer, received at least over $95 million in

Medicare reimbursements. Illumina caused the submission of those claims to Medicare.

## IV. THE FRAUDULENT SCHEME

49. Cybersecurity threats are caused by acts of individuals—whether intentional or unintentional. "The human element continues to drive breaches. [In 2022,] 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike." For this reason, companies like Illumina that do business with the Government are expected to comply with their promises to take measures to implement cybersecurity protections.

50. Illumina has represented that it "is committed to data security" and has the sophistication, expertise, technology, and resources to comply with its obligations under the QSR.

51. Based on its representations, the Government has funded Illumina genetic sequencing products and services ("products" is used broadly). Further, dozens of government agencies store their sensitive data and HIPAA-protected patient information on Illumina products. And dozens of lab companies use Illumina products to run genetic tests on behalf of Medicare beneficiaries. All of these customers also fund Illumina under servicing contracts for these products.

52. However, Illumina has knowingly ignored and minimized cybersecurity vulnerabilities in its products; failed to mitigate or correct known cybersecurity defects in its products, even resisting internal efforts to mitigate or correct the defects; and failed to disclose cybersecurity vulnerabilities to the Government. Therefore, the Government has not gotten what it paid for.

53. Illumina's knowing and continuing cybersecurity failures include:

- improper granting of elevated privileges to everyday users by default (analogous to having super admin rights of a database);
- failures to protect the credentials of everyday users by allowing their account user names and passwords to be generally accessible through hard coding of its software products (obviating the need for authentication and encryption before accessing or manipulating data); and
- failures to mitigate or correct the risk of insider threats.

54. Illumina prioritized developing and launching new products to beat the competition and maintain its dominant market share to the exclusion of basic cybersecurity protections for its products, which it has placed into the marketplace.

55. Because of these undisclosed cybersecurity defects, Illumina has knowingly continued to allow thousands of everyday users to have unauthorized access to its products, networks, and credentials (such as user names and

passwords), and to manipulate, supplement, and delete confidential patient data; change product configurations and settings; install unauthorized applications; grant third-parties access to the system; disable firewalls and other operating-system-level protections; enable external attacks on the system; and alter patient genomic test results—and to do so without detection.

56. Despite FDA's warning to product manufacturers to "implement comprehensive cybersecurity risk management programs" to "address the identification of security risks, the design requirements for how the risks will be controlled, and the evidence that the controls function as designed and are effective in their environment of use for ensuring adequate security," Illumina knowingly failed to meet the QSR design control requirements. And by knowingly failing to correct cybersecurity defects, it violated the QSR requirements which obligate manufacturers to "take appropriate and effective corrective and/or preventive action to prevent the[] recurrence" of "product and quality problems."

57. Illumina classifies cybersecurity issues using the industry-standard Common Vulnerability Scoring System ("CVSS"), a method developed by the National Institute of Standards of Technology ("NIST") to supply a qualitative measure of security. CVSS captures the principal technical characteristics of software, hardware, and firmware cybersecurity vulnerabilities. CVSS scores

thereby provide a universal metric to help organizations understand a vulnerability and determine the appropriate response, including vulnerability remediation.

58. The CVSS accounts for three types of metrics: base, temporal, and environmental. Base metrics represent the intrinsic qualities of a vulnerability—that is, the characteristics of a vulnerability that do not change over time or due to a user's environment. Temporal metrics reflect the characteristics of a vulnerability that change over time, measuring the current exploitability of a vulnerability and the availability of remediation. Environmental metrics allow an entity to modify a CVSS score to account for the special attributes of that entity's environment.

59. The base metrics create a CVSS score that ranges from 0 to 10:

0 = no severe vulnerability

0.1 to 3.9 = low-severity vulnerability

4.0 to 6.9 = medium-severity vulnerability

7.0 to 8.9 = high-severity vulnerability

9 to 10 = critically severe vulnerability

That base CVSS score is then modified by the temporal and environmental metrics to measure the ease and impact of exploitation of that vulnerability.

60. Illumina has knowingly launched genomic products with cybersecurity vulnerabilities that were assigned CVSS scores of 7.4 to 10 and continues to market and push its products with these high scores. Meanwhile,

Illumina continues to falsely certify to the Government that it is "committed to data security" and is complying with its obligations under the QSR.

61. Illumina's cybersecurity failures have been driven by its singular goal to maintain its dominant market presence. When faced with customer complaints related to the accessibility of data in its products, Illumina took fatal shortcuts. Rather than inconvenience customers and spend the necessary time and resources to properly address the issues raised by complaints, Illumina provided open access to all patient data to its customers with a quick flip-of-the-switch. In doing so, Illumina allowed expansive privileges to everyday customers, knowing that it was placing its products at high risk for cyberattack. In short, Illumina placed business needs ahead of providing the Government with the cybersecurity protections it certified. In the end, the Government did not get what it paid for.

### A. Certifying Products with Known Cybersecurity Vulnerabilities (Launch)

62. Illumina has launched and continues to sell products with known cybersecurity failures such as improper granting of elevated privileges to everyday users by default, hard coding of credentials to bypass authentication, and failures to mitigate insider threats.

63. As one example, Illumina launched the NovaSeq 6000Dx with known encryption and authentication deficiencies, which allowed individuals to access patient genetic data and controls without detection. And when made aware of

insider threats making this product vulnerable, it also knowingly failed to take steps to mitigate them. NIH has paid for this product for use in its All of Us program, the NIH Intramural Sequencing Center, the NIH National Institute on Aging, and the NIH National Cancer Institute.

64. Further, Illumina has continued to sell products with known cybersecurity failures including at least these products:

- NextSeq 1000 & 2000
- NovaSeq 6000 Series
- iSeq 100
- MiniSeq series
- NextSeq 550 Series
- iScan
- Off-instrument software

65. The Government has funded and used Illumina products, based on Illumina's certifications that patient data is protected from disclosure to insider and outsider threats. However, the Government did not get what it paid for.

66. Through its fraudulent course of conduct, Illumina knowingly submitted or caused to be submitted false or fraudulent claims under Government contracts, grants, and programs and Medicare claims, in violation of the False Claims Act, and the Government paid those claims.

### 1. Elevated Privileges

67. Only certain individuals within an organization should be given privileges. A "privilege is a special authorization that is granted to particular users to perform security relevant operations" such as authentication to access Illumina products.

68. A user with elevated privileges is one who "is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." They are afforded even greater authorization to access confidential patient data, delete files, modify systems, and grant malicious actors access to systems. Think of these as analogous to super admin rights. Elevated privileges afford a routine administrator greater rights and privileges. In the hands of the wrong authorized user with elevated privileges, cyber havoc can be wreaked on products.

69. Threat mitigation requires companies that house and use confidential and sensitive patient data to be judicious in granting elevated privileges. A common guideline in network security is the principle of least privilege, defined by NIST as "[t]he principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." That is, the principle of least privilege cautions that to

mitigate cybersecurity risks entities should grant users access to only the bare minimum of what they need to operate a product or system.

70. Yet Illumina has improperly allowed elevated privileges to users running genetic tests on Illumina products that are connected to an open network. These users include everyone—research assistants, third-party vendors, laboratory technicians, scientists, clinical investigators, engineers, and research and development staff —individuals who have no need for access to confidential and HIPAA-protected patient data including genomic test results. Further, this remains a known cybersecurity vulnerability, which Illumina has failed to mitigate or correct.

### 2. Exposed Credentials

71. Routine authentication protocol for users to access electronic systems and products, including usernames, passwords, tokens, or cryptographic key are called "secret keys" or credentials. The purpose of credentials to access electronic products is to ensure that users can authenticate their identities and are authorized to have access to the appropriate electronic data. "Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service."

72. However, Illumina hard-coded credentials, allowing users access to confidential patient data, without authentication. By hard coding credentials,

Illumina embedded credentials (e.g., usernames and passwords) into its software. "Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the product administrator."

73. Because users of Illumina products were authorized to access and manipulate confidential patient data without authentication, Illumina knowingly created cybersecurity vulnerabilities open to possible malicious actors without detection.

### 3. Insider Threats

74. Insider threats are commonplace. An insider is "[a]ny person with authorized access to any organizational resource, to include personnel, facilities, information, equipment, networks, or systems." An insider threat is "[t]he threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation."

75. Insider threats can be unintentional or intentional and are not necessarily malicious. Even unintentional threats can lead to breaches that may lead to confidential patient data getting in the hands of malicious actors.

76. Unintentional threats by insiders can lead to a data breach. For example, an insider may (a) decide to ignore internal security policies or directives

to install malware updates or security patches; (b) inadvertently forward confidential data to the wrong recipient; (c) open an attachment in a phishing email that contains a virus.

77. Intentional threats by insiders (or malicious actors) may also lead to a data breach through leaks of confidential data.

78. Illumina knows the risks posed by insiders. Its own onboarding training materials for employees discuss the possibilities of insider threats and the necessity for mitigation and action in response.

79. Yet Illumina ignored the known risks of insider threats despite internal and third-party reports that its products had known cybersecurity vulnerabilities including ones that Illumina itself caused. In doing so, Illumina knowingly allowed insider threats—both intentional and unintentional—to proliferate.

### B. Knowingly Failing to Mitigate or Correct Cybersecurity Vulnerabilities (Pre-Launch)

80. Illumina's knowledge of material cybersecurity failures long pre-dated the launch of its products and fall generally within three overlapping categories: improper granting of elevated privileges to everyday users, hard coding of credentials to bypass authentication, and failures to mitigate insider threats. In the limited instances in which Illumina did address cybersecurity failures, it did so only after complaints from third parties that malicious actors had exploited

vulnerabilities in its products. Further, mitigation was incomplete and failed to disclose the scope of the vulnerabilities.

81. For example, in January 2016, an associate professor at the University of Pennsylvania's School of Veterinary Medicine ("UPenn") reported that multiple Illumina products used by the school were victimized by a ransomware attack. Despite evidence that the UPenn account had been hacked, the professor reported that Illumina "specifically instructed" him not to change his log-in information following the attack.

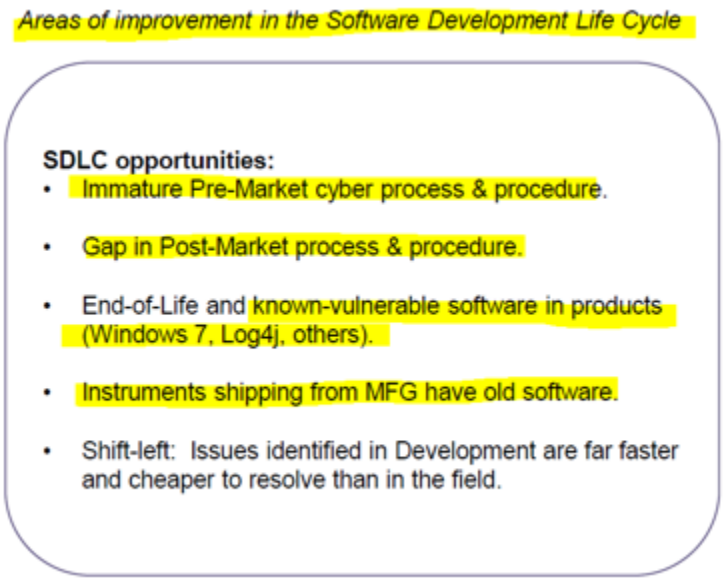
82. As another example, in September 2018, a professor in the Department of Ecology and Evolutionary Biology at the University of California, Santa Cruz reported that Illumina's MiSeq product was victimized by a separate ransomware attack.

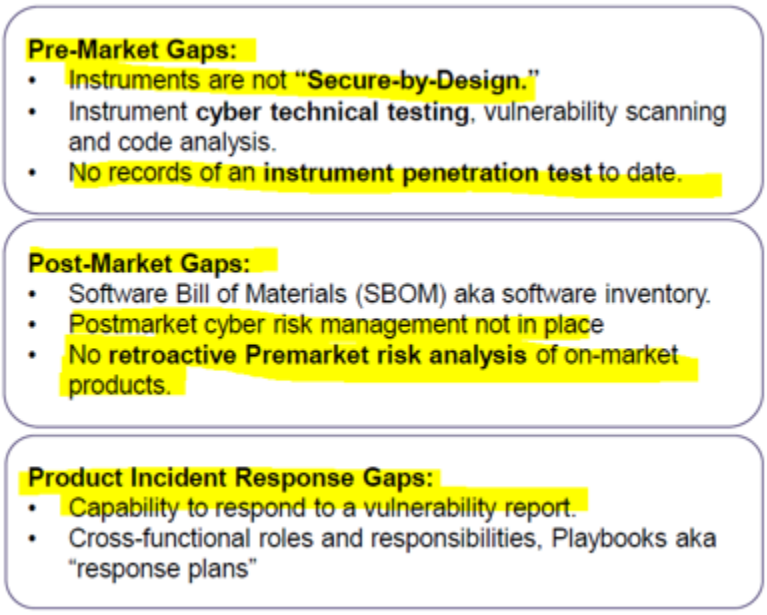
83. Cybersecurity vulnerabilities of its products were discussed at high-level meetings within Illumina, but senior management failed to take corrective action in response. One such meeting took place on April 20, 2022, in which senior members of management discussed cybersecurity deficiencies and insufficient safeguards alleged in this Complaint ("Q1 2022 On-Market All-Hands Meeting").

84. The Q1 2022 On-Market All-Hands Meeting took place remotely through Microsoft Teams. The Director of Product Security prepared and

delivered the portion of the presentation on the product and cybersecurity program with the Vice President of R&D Operations and Portfolio Management, the Global Head of Software and Informatics, and the Chief Operating Officer in attendance at the meeting.

85. At the meeting, the Director acknowledged known cybersecurity vulnerabilities in its products:






86. Illumina products were described as not "Secure-by-Design." Further, despite its certifications to the Government, Illumina knowingly failed to perform penetration tests prior to launch of its products.

87. Descriptions of known post-market vulnerabilities included failures in cybersecurity management and cyber-technical testing, vulnerability scanning, and code analysis of its products, along with the failure to perform retroactive pre-market risk analysis of on-market products. The Director of Product Security also highlighted Illumina's complete failure to respond to vulnerability reports, which contain a review of cybersecurity weaknesses in the products.

88. Further, routine cybersecurity protections to create a "minimal viable product"—one that meets customer expectations and complies with Government requirements—were also proposed at the Q1 2022 On-Market All-Hands Meeting.

These recommendations included cybersecurity risk assessments of products in the pre-market phase such as threat modeling and cyber-technical and penetration testing; and cybersecurity risk assessments of products in the post-market products phase such as vulnerability technical scanning and monitoring and cyber-surveillance. However, Illumina has failed to act on these recommendations despite its certifications to the Government to the contrary.

89. The Government has funded and used Illumina products, based on Illumina's certifications that it would mitigate or correct known cybersecurity vulnerabilities. However, the Government did not get what it paid for.

90. Through its fraudulent course of conduct, Illumina knowingly submitted or caused to be submitted false or fraudulent claims under Government contracts, grants, and programs and Medicare claims, in violation of the False Claims Act, and the Government paid those claims.

### 1. Elevated Privileges

91. Since at least as early as 2019, Illumina has knowingly allowed thousands of everyday users of its products to have elevated privileges, which has made its products highly vulnerable to cyberattacks.

92. Yet Illumina made disclosures of possible data breaches to the Government under limited circumstances in the form of two recalls: the 2022 Local Run Manager (LRM) recall and the 2023 Universal Copy Service (UCS)

recall. The vulnerability caused by elevated privileges disclosed in the LRM recall was assigned a CVSS score of 10 (a critically severe vulnerability) and in the UCS recall was assigned a CVSS score of 7.4 (a high-severity vulnerability).

93. Further, Illumina's representations in these limited and untimely recalls were only half-truths because, while Illumina knew that the same vulnerabilities caused by the improper allowance of elevated privileges (a) had not been eliminated in these two recalled products and (b) existed in other Illumina products, it failed to make these disclosures to the Government or to recall other products.

**a. In 2019 and 2020, Illumina Removed Safeguards from its LRM Software**

94. At least as early as 2019, users had problems accessing Illumina's Local Run Manager ("LRM") software, a proprietary software that manages genetic sequencing runs and analyzes data, because they were getting administratively locked out of the system. To address this inconvenience to customers, Illumina disabled a function that served as a basic cybersecurity safeguard to properly limit user access. As a result, all LRM users were granted elevated privileges, which allowed them unauthorized access to Illumina products, networks, and credentials (user names and passwords), and to manipulate, supplement, and delete confidential patient data; change product configurations and settings; install unauthorized applications; grant third-parties access to the

system; disable firewalls and other operating-system-level protections; enable external attacks on the system; and alter patient genomic test results. Thus, Illumina knowingly caused its product to be vulnerable to data breaches to mollify customers.

95. In April 2020, Illumina performed a design failure mode and effect analysis ("April 2020 Design FMEA"), which is an analysis of potential risks introduced in a product through a new or changed design —a minimal cybersecurity check of its products. FDA requires design validation to include risk analysis for all products. The analysis uncovered that Illumina provided elevated privileges that allowed users to change the storage location of confidential patient data including test results, thereby allowing them to save data locally (e.g., on their personal desktop or a removable drive) rather than on the Illumina product. Yet again, Illumina knowingly caused its product to be vulnerable to data breaches to mollify customer complaints related to basic use of its products.

**b. In October 2021, Customer Discovered Cybersecurity Vulnerabilities in LRM Software**

96. In October 2021, Roche, the pharmaceutical company, a sizeable Illumina customer, also contacted Illumina regarding cybersecurity vulnerabilities it had identified in the LRM software as the result of a routine penetration test that Roche conducts on products it uses. Penetration testing is "[a] test methodology in which assessors, typically working under specific constraints, attempt to

circumvent or defeat the security features of a system." Essentially, penetration testing is a stress test of a program designed to assess whether the program is vulnerable to cybersecurity hacks.

97. Notably, Illumina failed to conduct its own penetration testing of the LRM software even though it certified to the Government that it has conducted cybersecurity testing of its products.

**c. In August 2022, Illumina Recalled LRM Software for First Time**

98. In August 2022, through a recall, Illumina first disclosed to the Government the cybersecurity vulnerabilities in its LRM software caused by its improper granting of elevated privileges to everyday users—nearly one year after Roche's finding and notification to Illumina ("LRM recall"). Illumina assigned a CVSS score of 10—denoting a critically severe vulnerability.

99. The same recall also disclosed for the first time that Illumina failed to implement basic cybersecurity safeguards such as authentication and encryption. These failures were assigned a CVSS score of 9.1—critically severe vulnerabilities.

100. However, the LRM recall itself was a half-truth because at the time of the recall, Illumina was aware that the same vulnerabilities caused by the improper allowance of elevated privileges existed in other Illumina products—both on-

market products and those about to be launched—but knowingly failed to recall those products as well.

**d. In 2023, Illumina Recalled UCS Software Caused by Removal of Same Safeguard.**

101. In April 2023, through another cybersecurity recall, Illumina first disclosed to the Government the cybersecurity failures in certain versions of its UCS software. The UCS is a software used in Illumina medical products to ensure that the results of genetic testing are copied from a product's local file folder to a folder on the cloud.

102. The recall notified customers that Illumina products running versions one and two of the UCS contained "an unnecessary privileges vulnerability" which allowed "[a]n unauthenticated malicious actor" to "upload and execute[] code remotely at the operating system level, which could allow an attacker to change settings, configurations, software, or access sensitive data on the affected products."

103. However, this recall was also a half-truth like the LRM recall because, Illumina remained aware that the same vulnerabilities that led to the LRM and UCS recalls caused by the improper allowance of elevated privileges still existed in other Illumina products—both on-market products and those about to be launched—but knowingly failed to recall those products as well. The same material cybersecurity vulnerabilities remain at large in other Illumina products.

### 2. Exposed Credentials

104. For at least two years, Illumina has knowingly exposed credentials in the plain text of its coding. On information and belief, Illumina has taken no steps to remedy this outstanding cybersecurity vulnerability, thereby exposing confidential patient data including test results to anyone with access to Illumina products including possible malicious actors.

#### a. In 2020, Illumina Test Revealed Improper Hard Coding of User Credentials in its Product.

105. In February 2020, Illumina performed a software hazard analysis of its NovaSeq product, a basic cybersecurity test to determine whether the software satisfies system safety design criteria. The analysis revealed that the "secret access key [e.g., usernames and passwords] for S3 [is] displayed as plain text in [the] run parameters" of the NovaSeq. Said more plainly, Illumina improperly hard-coded credentials used to access confidential patient genomic data stored in the cloud, allowing everyday users to see the login information in plain text. The cloud services for users are provided by Amazon Web Services ("AWS") and were intended to provide "genomic analysis customers with secure, cloud-based data processing, management, and storage." Thus, contrary to Illumina's certifications to the Government, this material cybersecurity failure made confidential patient

data including test results vulnerable to breach. Further, on information and belief, Illumina failed to disclose this vulnerability to the Government.

**b. As Late as 2022, Third Party Uncovered Continued Hard Coding of Illumina Product**

106. In August 2022, another third-party vendor (Veracode) notified Illumina of further cybersecurity vulnerabilities it had identified in two routine static scans (i.e., review source code to find product cybersecurity failures), which it performed on Illumina products.

107. Veracode is the creator of RabbitMq, a software product used by Illumina that helps applications and systems communicate with one another. Veracode uncovered that Illumina had improperly hard-coded credentials (e.g., usernames and passwords) for use with RabbitMq and that this cybersecurity vulnerability was "likely" exploitable. In response to the first static scan, Illumina admitted that RabbitMq contained hard-coded credentials, which it used for unit tests of its products (i.e., diagnostic tests to evaluate whether products are functioning properly), despite knowing that hard coding of credentials increases the risk of data breaches.

108. And this remains a known cybersecurity vulnerability even after the LRM recall.

### 3. Insider Threats

109. Since at least 2020, Illumina has known of cybersecurity vulnerabilities in its products that may have resulted from insider threats. Yet Illumina failed to take steps to investigate or mitigate these risks or correct known cybersecurity vulnerabilities.

#### a. Illumina Minimized Insider Threats Uncovered by 2020 LRM Analysis

110. Instead of taking steps to mitigate known vulnerabilities in response to its April 2020 modes and effects analysis of its LRM software, Illumina improperly concluded that "the intended users are lab scientists/informed users [who] will not maliciously configure these settings," thereby ignoring the risks posed by insider threats.

#### b. August 2022 Third Party Report Confirmed Continued Insider Threat Risk

111. The August 2022 Veracode Report uncovered that the NovaSeq6000Dx was vulnerable to insider threats. The first scan detected numerous cybersecurity vulnerabilities including those related to directory traversal, a web-security vulnerability that allows an attacker to gain unauthorized access to confidential data and to take control of a server. According to the report, while Illumina superficially attempted to mitigate the directory traversal flaws to

minimize the cybersecurity risk, there was still a "[r]emaining [r]isk" that the vulnerability "still can be hacked by [an] Illumina insider."

112. On information and belief, Illumina failed to mitigate the known insider threat vulnerabilities to NovaSeq 6000Dx before launch of the product on September 29, 2022; and failed to notify the Government of the known cybersecurity vulnerabilities.

113. Further, Illumina certified to the Government that it performed penetration testing, acknowledging that "[t]he Veracode (SAST) static scan is NOT sufficient for software security validation." However, despite its promises, Illumina performed only the static scan—the most basic form of software security scanning—and failed to perform penetration testing as promised.

**c. September 2022 NovaSeq 6000Dx Cyber Report Again Confirms Risk of Insider Threats**

114. Further, in mid-2022, an Illumina NovaSeq 6000Dx cybersecurity report disclosed that "the most likely attacker profile for the product is a disgruntled ex- or current staff member, with access to the LAN network." Despite this knowledge, Illumina still launched the product three days later and failed to mitigate the cybersecurity vulnerability or provide notice to the Government.

115. On information and belief, Illumina still has not mitigated the known cybersecurity vulnerabilities in NovaSeq 6000Dx products, which the Government continues to use.

### C. Material Violations of Government Requirements

116. Illumina knew that compliance with the laws and regulations set forth in this Complaint was material to the Government's decision to pay directly or indirectly for use of Illumina genetic sequencing products under Government contracts, grants, and programs, and for Medicare claims for genetic testing. Illumina also knew that truthful records and statements in support of payments under Government contracts, grants, and programs and Medicare claims were material to the Government's decision to pay these claims.

117. Some of the factors in evaluating materiality under the False Claims Act include (a) statutory, regulatory, and contractual language, (b) whether the violations go to the heart of the benefit of the bargain, (c) whether the violations were serious and material and not merely technical or minor infractions of rules, (d) the Government's actions relative to similar violations, (e) whether any reasonable person would attach importance to Defendant's choice of actions, and (f) Defendant's knowledge relative to these factors. All these factors demonstrate materiality in this case and have been addressed throughout this Complaint.

118. Illumina knowingly made false representations and certifications that caused the Government to pay directly or indirectly for use of Illumina genetic sequencing products and Medicare claims. Illumina knowingly submitted or caused to be submitted thousands of false or fraudulent claims for payment

including Medicare claims and used false records and statements in support of payments under Government contracts, grants, and programs and Medicare claims.

119. Illumina's failure to mitigate known cybersecurity vulnerabilities in its products not only harmed its customers and patients but were material violations of requirements in federal regulations and Government contracts.

120. Under the QSR's design control regulations, Illumina was required to establish and maintain procedures for validating product design, including software validation and risk analysis. Manufacturers like Illumina can comply with this requirement by implementing comprehensive cybersecurity risk management programs. 21 CFR § 820.30(g).

121. Yet Illumina failed to comply with the QSR's design control regulations because of its inadequate pre-market cybersecurity risk management programs. Illumina itself acknowledged internally that cybersecurity gaps in its products during the pre-market stage included the fact that they were not "secure-by-design" and were not properly tested through standard means (cyber-technical testing, vulnerability scanning, code analysis, penetration testing). Because of its failure to adequately pre-market test its products, Illumina launched products such as the NovaSeq 6000Dx with known material cybersecurity failures.

122. Under the QSR's corrective and preventative action regulations, Illumina was required to identify and investigate any problems (including quality)

with its products and take appropriate and effective corrective and preventive action, as necessary. The FDA has reinforced to medical device manufacturers like Illumina that implementation of comprehensive cybersecurity risk management programs, and documentation of such, are material to compliance with CAPA requirements. 21 CFR § 820.100(a).

123. However, Illumina failed to implement (or document) comprehensive cybersecurity risk management programs to demonstrate compliance with the QSR regulations. To the contrary, Illumina failed to implement either pre/post-market cybersecurity risk management or retroactive pre-market risk analysis of on-market products. Various reports prepared by Illumina and third parties over the past several years have shown material cybersecurity failures in Illumina products on the market. It was only when market participants called out cybersecurity failures in Illumina products that Illumina issued superficial recalls of certain products, i.e., the LRM and UCS recalls. Through these recalls, Illumina made disclosures of cybersecurity vulnerabilities that contained half-truths. The recalls were half-truths for at least two reasons: (a) they were limited to two products instead of all products containing the same known vulnerabilities; and (b) they failed to disclose all vulnerabilities such as the improper hard coding of credentials and others that exposed the products to insider threats.

124. Under the QSR's management regulations, Illumina management—"those senior employees of a manufacturer who have the authority to establish or make changes to the manufacturer's quality policy and quality system"—is responsible to ensure that the quality system is both implemented and effective. 21 CFR §§ 820.20(a) and 820.3(n).

125. Yet Illumina management failed to ensure that its quality system was implemented and effective. Far from it. Instead, management actively discounted, disregarded, and suppressed attempts by Illumina employees to raise and address material cybersecurity vulnerabilities.

126. Further, under the QSR, Illumina was required to "establish and maintain procedures to control product that does not conform to specified requirements." Through these procedures, it must "address the identification, documentation, evaluation, segregation, and disposition of nonconforming product." 21 C.F.R. § 820.90(a).

127. Illumina failed to control for nonconforming products. Rather, Illumina launched products with known vulnerabilities on the market with no warnings to customers—including Government customers and companies that handle sensitive data of Government-insured beneficiaries—that its products were plagued by material cybersecurity failures.

128. Because Illumina is the only entity authorized to perform maintenance on Illumina products, once the Government (or company) purchases an Illumina product, the customer is tied to Illumina for servicing contracts for the operating life of the product. As part of its servicing contracts with the Government (and companies), Illumina was required to provide preventative hardware maintenance and proprietary software maintenance and upgrades. By failing to mitigate and correct known cybersecurity failures in its products, Illumina knowingly violated these contracts with the Government and other companies.

129. As part of its partnership with the NIH through its All of Us Research Program, Illumina was expected to comply with program rules for privacy and data security. NIH provides notification to its partners of ways in which they can comply with the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 ("NIST Framework"). The NIST framework establishes a guide using five functions—Identify, Protect, Detect, Respond, and Recover—to enable an entity to assess cybersecurity and data security performance. These include security measures to identify, assess, and respond to vulnerabilities and threats; and contain security incidents; and compliance with applicable laws and regulations. However, Illumina failed to safeguard its products or comply with these cybersecurity requirements; and knowingly

concealed material cybersecurity vulnerabilities in products used by the All of Us Program.

130. Further, several private laboratories rely on Illumina products to carry out genetic testing for which they seek Medicare reimbursement. Foundation Medicine and Myriad are two such labs that have received over $250 million in Medicare reimbursement to treat and diagnose Medicare patients. Illumina products they have relied upon contain the same material cybersecurity vulnerabilities, which threaten the integrity of the testing data produced by the products and could lead to data breaches.

131. This case is precisely the type of fraud scheme remedied by the False Claims Act. One example is *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings*:

> These acquisition regulations require that the defense contractor undertake cybersecurity specific measures before the contractor can handle certain technical information. Here, compliance with these cybersecurity requirements could have affected AR's ability to handle technical information pertaining to missile defense and rocket engine technology. Accordingly, misrepresentations as to compliance with these cybersecurity requirements could have influenced the extent to which AR could have performed the work specified by the contract. (internal citations omitted)

*U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc*., Memorandum and Order Re: Defendants' Motion to Dismiss, 381 F. Supp. 3d 1240, 1248 (E.D. Cal. 2019).

132. In July 2022, after the summary judgment decision in favor of plaintiff, Aerojet Rocketdyne agreed to pay $9 million to resolve allegations by a former employee that Aerojet violated cybersecurity requirements in federal government contracts, including with DOD and NASA. Press Release, *Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts* (July 8, 2022), https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity

133. In speaking about the Aerojet settlement, DOJ Principal Deputy Assistant Attorney General Brian M. Boynton recognized that "[w]histleblowers with inside information and technical expertise can provide crucial assistance in identifying knowing cybersecurity failures and misconduct." Press Release, *Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts* (July 8, 2022), https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity

134. The United States also filed a "statement of interest" supporting the plaintiff's summary judgment briefing that led to a favorable decision for the plaintiff. *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Memorandum and Order Re: Cross Motions for Summary Judgment, No. 2:15-cv-02245 WBS

AC, 2022 WL 297093 (E.D. Cal. Feb. 1, 2022) (slip op.); United States' Statement of Interest in Connection with Defendants' Summary Judgment Motion, *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245 (Oct. 20, 2021), https://www.onlineandonpoint.com/wp-content/uploads/sites/40/2022/02/Aerojet-Statement-of-Interest.pdf

135. In denying the defendants' motion for summary judgment, the Court found that "[i]t may be reasonably inferred that compliance [with FAR clauses mandating cybersecurity protections] was significant to the government because without complete knowledge about compliance, or noncompliance, with the clauses, the government cannot adequately protect its information." *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Memorandum and Order Re: Cross Motions for Summary Judgment, No. 2:15-cv-02245 WBS AC, 2022 WL 297093, at *7 (E.D. Cal. Feb. 1, 2022) (slip op.).

136. In a different case, in March 2022, a medical services contractor agreed to pay nearly $1 million to resolve allegations that it falsely represented to the U.S. State Department and the U.S. Air Force that it would use a secure electronic medical records system in providing medical services to U.S. military service members, diplomats, officials, and contractors working in certain conflict zones, to protect the confidentiality of their health information and PII. The contractor's failure to utilize a secure system exposed sensitive medical records

and PII to non-clinical staff. Again, the DOJ Principal Deputy Assistant General stated, "This settlement demonstrates the department's commitment to use its civil enforcement tools to pursue government contractors that fail to follow required cybersecurity standards . . . We will continue to ensure that those who do business with the government comply with their contractual obligations, including those requiring the protection of sensitive government information." Press Release, *Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts in State Department and Air Force Facilities in Iraq and Afghanistan* (Mar. 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical

137. Further, in July 2019, a contractor agreed to pay $8.6 million to resolve allegations that it knowingly sold flawed video surveillance systems to federal and state government entities that *may* have but did not actually result in the disclosure of information. Press Release, *Attorney General James Secures $6 Million from Cisco Systems in Multistate Settlement* (Aug. 1. 2019), https://ag.ny.gov/press-release/2019/attorney-general-james-secures-6-million-cisco-systems-multistate-settlement; *Cisco to Pay $8.6 Million to Settle Government Claims of Flawed Tech*, N.Y. TIMES (July 31, 2019), https://www.nytimes.com/2019/07/31/technology/cisco-tech-flaw-sales.html

138. In an earlier case, in November 2015, a contractor and subcontractor responsible for implementing software to manage the DOD's telecommunications network collectively agreed to pay $12.75 million to resolve allegations that they allowed unauthorized access to sensitive government data by using individuals on the contract who lacked the requisite security clearances. Press Release, *Netcracker Technology Corp. and Computer Sciences Corp. Agree to Settle Civil False Claims Act Allegations* (Nov. 2, 2015), https://www.justice.gov/opa/pr/netcracker-technology-corp-and-computer-sciences-corp-agree-settle-civil-false-claims-act

139. Cybersecurity vulnerabilities in medical products including devices are a growing threat. On September 12, 2022, the FBI warned that it had identified an increasing number of cybersecurity vulnerabilities "posed by unpatched medical devices that run on outdated software and devices that lack adequate security features." The FBI explained that "[m]edical devices vulnerabilities predominantly stem from device hardware design and device software management," and that further, when malicious actors exploit cybersecurity vulnerabilities in medical devices, they harm the ability of health care facilities to operate, jeopardize patient safety, and compromise data confidentiality and data integrity.

140. As part of the Government's attempt to combat these and similar cybersecurity threats, the Biden Administration unveiled a national cybersecurity strategy calling for a more aggressive approach to addressing cybersecurity vulnerabilities: "malicious cyber activities continue to threaten Americans across society, including disproportionately affecting those without the resources necessary to protect themselves, recover, or seek recourse." To ensure a more secure future, the current Administration announced cybersecurity requirements and performance-based regulations in critical sectors and a stated intention to work with Congress to close gaps in the authority of federal departments and agencies to implement minimum cybersecurity requirements and mitigate related market failures.

141. The Administration also emphasized that a more secure digital landscape cannot be achieved by federal government intervention alone and stressed that, "we must ask more of the capable and best-positioned actors to make our digital ecosystem secure and resilient," noting that "[t]he private sector is capable of mitigating most cyber incidents without direct Federal assistance." Elaborating on this point, "[i]n a free and interconnected society, protecting data and assuring the reliability of critical systems must be the responsibility of the owners and operators of the systems that hold our data . . . as well as of the technology providers that build and service these systems" and "[a]ll service

providers must make reasonable attempts to secure the use of their infrastructure against abuse or other criminal behavior."

142. The Director for the HHS-Office of Civil Rights ("OCR") has stressed "why it is so important for health care to be vigilant in their approach to cybersecurity": "unpatched vulnerabilities give hackers access to an organization's computer server, and possible entry into other parts of a network." Because of this threat, the Director of OCR called on companies to "strengthen [their] organization's cyber [posture]." In particular, the Director highlighted best practices, including "[c]onducting regular scans to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface;" and "[r]egular patches and updates of software and Operating Systems."

143. The False Claims Act cases and numerous public pronouncements by HHS, DOJ, including during the current Administration, demonstrate that Illumina's conduct alleged in this Complaint was material to the Government's decision to pay claims.

144. The facts alleged in the Complaint show that Illumina was well aware of the statutory and regulatory requirements pled here; and, further, that the violations alleged in this Complaint were material to the Government's decision to fund Illumina products under Government contracts, grants, and programs and to pay Medicare claims for genetic testing.

145. Illumina also well knew that the unlawful conduct alleged in this Complaint went to the very heart of the bargain of its Government contracts, grants, and programs for Illumina products and its payment of Medicare claims for genetic testing. The Government expects and requires that claims be paid only for accurate and truthful Medicare claims and under Government contracts, grants, and programs.

146. Illumina's statutory, regulatory, programmatic, and contractual requirements for complete, accurate, and truthful reporting during the claims submission process also go directly to the "essence of the bargain." These requirements are neither "minor nor insubstantial."

147. Illumina's violations of the statutory, regulatory, programmatic, and contractual requirements were serious and material, leading to actual or potential harm, and were made with at least reckless disregard of the seriousness of the violations.

148. Illumina's violations were not immaterial or inadvertent technical mistakes in processing paperwork, or simple and honest misunderstanding of the rules, terms and conditions, or certification requirements. Rather, Illumina knowingly failed to comply with material legal obligations and certifications.

149. Illumina knew that it was submitting or causing to submit false or fraudulent claims for, and false or fraudulent statements, records, and tainted

claims under Government contracts, grants, and programs and for Medicare reimbursement, which the Government paid.

150. In short, there is ample evidence to show that Illumina knew or should have known that its violations had the natural tendency to influence the Government's decision to pay claims under Government contracts, grants, and programs and Medicare claims for genetic testing and that any reasonable person would attach importance to Illumina's choice of action.

**D. Scienter**

151. Illumina has known that its cybersecurity failures are widespread, and that confidential patient data is highly vulnerable to breach despite its certifications to the Government to the contrary. Further, Illumina has knowingly chosen to disregard these serious risks and failed to take steps to mitigate these problems.

152. Illumina senior management is aware that its products at launch and in the marketplace do not have the cybersecurity protections promised to the Government. Illumina has knowingly failed to perform routine cybersecurity testing such as penetration and other technical testing and vulnerability scanning before launch of its products. Once on the market, Illumina has knowingly failed to manage its cybersecurity risks or perform analyses of its products.

153. In 2016 and 2018, at least two outside sources reported ransomware attacks by malicious actors who exploited known vulnerabilities in Illumina

products caused by Illumina's failure to implement basic cybersecurity protections promised to the Government. Illumina failed to mitigate and in one known instance "specially instructed" the outside source to not change his log-in information following the attack.

154. More recently, in August 2022, members of Illumina's Product Security Team attended a hacking event in Las Vegas called DEF CON 30. One attendee demonstrated for the Illumina team that they were able to hack its iSeq product in only 15 minutes, thereby breaching the data contained on its product. That same month a third party conducting a penetration test also revealed material cybersecurity vulnerabilities.

155. Illumina's Product Security Team, proceeding under its written quality management procedure, escalated the known cybersecurity vulnerabilities to Illumina management within numerous departments. Senior management within at least two departments (R&D Operations and Portfolio Management and Global Software and Informatics) took steps to prevent mitigation, including directing the Product Security Team to ignore written policies to address mitigation, not convene a risk determination meeting with other departments, and not involve the legal department.

156. With knowledge of these material cybersecurity failures, Illumina failed to mitigate and failed to disclose them to the Government. Instead, Illumina

launched the NovaSeq 6000Dx with a known CVSS score of 7.4 (high-severity vulnerability).

## V. UNLAWFUL RETALIATION

157. Relator was employed at Illumina as the Associate Director and then Director of Portfolio and Program Management, On-Market Products from May 4, 2020, to September 1, 2022. During this time, Relator was troubled that Illumina was engaged in the unlawful practices alleged in this Complaint. Relator also feared job security and the legal propriety of Illumina's actions. Relator repeatedly and consistently informed management of concerns related directly to the allegations set forth in the Complaint and urged management to create a product security function.

158. Yet Relator was continually ignored, reprimanded, marginalized, and retaliated against by Illumina for raising concerns related to, and objecting to, Illumina's fraudulent course of conduct alleged in this Complaint. Relator was ultimately discharged by Illumina for raising these concerns.

159. Illumina retaliated against and discharged Relator because of lawful acts by Relator to stop one or more violations of the False Claim Act and lawful acts by Relator in furtherance of an action under 31 U.S.C. § 3730. On September 1, 2022, Relator was terminated because of lawful acts by Relator to stop one or

more violations of the False Claim Act and lawful acts by Relator in furtherance of an action under 31 U.S.C. § 3730.

160. The following summarizes certain events that occurred in addition to those alleged throughout the Complaint.

161. Relator is a respected professional in the field of life sciences technologies and was hired by Illumina to oversee all of Illumina's on-market products. Shortly after working for Illumina, Relator was promoted based on the recommendation of her then-supervisor, the Senior Director of On-Market Portfolio.

162. During her time at Illumina, Relator addressed numerous cybersecurity problems in Illumina products and managed multiple product recalls including those alleged in this Complaint.

163. Relator worked tirelessly for the company, even spending significant portions of her paid vacations to address and attempt to remedy Illumina's seemingly endless cybersecurity crises.

164. In July 2020, within months of Relator joining Illumina, Relator led a working group ("OS Security Tiger Team") that assembled to address operating-system issues and other software-related complaints across various Illumina products. The OS Security Tiger Team determined that Illumina products were plagued by significant cybersecurity gaps. Notably, the OS Security Tiger Team

learned that Illumina had not run a single penetration test on any of its products. The same team further learned that Illumina had a security inbox set to receive product security complaints which no one checked, and which contained, among other messages, an email from the U.S. Department of Homeland Security notifying Illumina of cybersecurity vulnerabilities in the company's products.

165. Having learned of Illumina's deficient cybersecurity safeguards and insecure products, members of the OS Security Tiger Team—including Relator—escalated their concerns to R&D management on multiple occasions. In at least two quarterly sPAC ("Strategy, Product Approval Committee") strategy meetings with senior leadership, Relator voiced concerns about the cybersecurity vulnerabilities of Illumina products and the lack of a product security function at Illumina.

166. In July 2021, Relator's supervisor, the Senior Director of On-Market Portfolio transitioned to another job. As a result, the Vice President of R&D Operations and Portfolio Management promoted Relator to the interim position of overseeing the entire On-Market Products Portfolio. Relator accepted and served in this role until October 2021. In this additional role, Relator oversaw a staff of approximately 28 individuals, which included Platform Management Teams (PMTs), Technical Leads, Program Managers, and Global Product Support

employees (GPS). Relator also attended the sPAC meetings and was assigned many additional responsibilities.

167. In August 2021, Relator was promoted to the position of Director of Portfolio and Program Management, On-Market Products.

168. In October 2021, only after several employees—including Relator—repeatedly expressed their concerns about cybersecurity vulnerabilities in its products, Illumina created a product security function and put in place a Director of Product Security with a skeleton staff.

169. In January 2022, the then-Senior Director of On-Market Portfolio asked Relator to assume yet another role as interim Technical Lead of Mid-Throughput Instruments. In this additional role, Relator oversaw the NextSeq 550 Dx, NextSeq 550, and MiniSeq platforms.

170. In January 2022, the Senior Director of On-Market Portfolio asked Relator to lead two FDA recalls—the NextSeq platform recall related to issues with short circuiting and thermal events, and the LRM recall. Over the course of the next several months, Relator successfully led and completed both recalls. This was no small task. The LRM recall was Illumina's largest recall to date, impacting approximately 16,000 instruments and six platforms.

171. By end of January 2022, Relator was playing four separate roles at Illumina—essentially doing the jobs of four people. Relator was serving as

Director of Portfolio and Program Management, On-Market Products, acting as the interim Technical Lead of Mid-Throughput Instruments, and leading two separate FDA recalls. Nevertheless, Relator successfully balanced the added responsibilities. Relator received at least four or five bonuses for her work during this time.

172. In early August 2022, the Director of Product Security noted the existence of critically severe cybersecurity vulnerabilities in Illumina products. Relator repeatedly tried to initiate quality investigation ("QI") meetings to address these vulnerabilities with Illumina's Quality, Legal, Regulatory, Product Security, and R&D Departments.

173. The Vice President of R&D Operations and Portfolio Management and the Global Head of Software and Informatics, however, repeatedly thwarted Relator's attempts to properly investigate and remediate the material cybersecurity vulnerabilities and directed Relator and the Director of Product Security to cancel investigative meetings. For example, Relator scheduled a QI meeting and invited key individuals from other functions such as Quality and Regulatory and the Director of Product Security, pursuant to the QI process. However, the Vice President of R&D Operations and Portfolio Management and the Global Head of Software and Informatics canceled the meeting, instead scheduling a private meeting with Relator. According to the VP and Global Head, they wanted to keep

the identified cybersecurity vulnerabilities confidential and "within R&D." Relator avoided meeting with them privately out of fear they intended to use the meeting to pressure Relator to take unethical actions or remain quiet about the cybersecurity vulnerabilities.

174. Upon learning of this conduct, the Vice President of Global Quality and Compliance recommended that Relator report these events to the Compliance Department. Within hours of this conversation, the Vice President of R&D Operations and Portfolio Management informed Relator that Relator would no longer be managing the identified cybersecurity vulnerabilities. The Associate Director of Technical Program Management was given authority over the cybersecurity concerns and Relator was abruptly excluded from all future activities and discussions. When Relator spoke with the Associate Director about her exclusion from these meetings and activities, the Associate Director informed Relator that she was uncomfortable sharing information with Relator regarding discussions about cybersecurity vulnerabilities.

175. Relator reported these allegations to the Compliance Department, which opened an investigation, and was told the Chief Compliance Officer would be informed of Relator's report. Members of the Compliance Department assured Relator that she would not experience retaliation and that Illumina adhered to strict whistleblower protections. Despite these assurances, on September 1, 2022, the

Vice President of R&D Operations and Portfolio Management terminated Relator by videoconference. The Senior Director of On Market Portfolio and a Human Resources employee were both on the call. When Relator asked for the reason for her termination, the Vice President of R&D Operations and Portfolio Management told Relator that the termination was due to restructuring and that her termination was not related to Relator's job performance.

## VI. COUNTS

### COUNT I

### Federal False Claims Act: 31 U.S.C. § 3729(a)(1)(A)

176. The allegations in the preceding paragraphs are incorporated by reference.

177. Defendant knowingly presented or caused to be presented false or fraudulent claims for payment or approval in violation of 31 U.S.C. § 3729(a)(1)(A).

178. The United States paid for claims that otherwise would not have been allowed.

179. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus

civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

180. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

## COUNT II

### Federal False Claims Act: 31 U.S.C. § 3729(a)(1)(B)

181. The allegations in the preceding paragraphs are incorporated by reference.

182. Defendant knowingly made, used or caused to be made or used, false records or statements material to false or fraudulent claims, in violation of 31 U.S.C. § 3729 (a)(1)(B).

183. The United States paid for claims that otherwise would not have been allowed.

184. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

185. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

## COUNT III

### Federal False Claims Act: 31 U.S.C. § 3729(a)(1)(G)

186. The allegations in the preceding paragraphs are incorporated by reference.

187. Defendant knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money or property to the Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money or property to the Government, in violation of 31 U.S.C. § 3729 (a)(1)(G).

188. The United States paid for claims that otherwise would not have been allowed.

189. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

190. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

## COUNT IV

### Retaliation of Relator in Violation of False Claims Act 31 U.S.C. § 3730(h)

191. The allegations in the preceding paragraphs are incorporated by reference.

192. Relator engaged in lawful acts in furtherance of efforts to stop one or more violations of 31 U.S.C. § 3729.

193. Because of Relator's lawful acts, Relator was subjected to retaliation by Defendant.

194. Relator was unlawfully retaliated against by Defendant and for engaging in protected activity, namely for raising, objecting to and refusing to participate in fraudulent conduct alleged in this Complaint.

195. Defendant's retaliation against Relator was a violation of 31 U.S.C. § 3730(h).

196. As a result of Defendant's violations of 31 U.S.C. § 3730(h), Relator suffered damages.

197. Relator is entitled to damages sustained as a result of the retaliation, including litigation costs and reasonable attorneys' fees, and all other remedies and recompense allowable under 31 U.S.C. § 3729(h).

**WHEREFORE**, Relator, on behalf of Relator and the United States, pray:

(a) That the Court enter judgment against Defendant in an amount equal to three times the amount of damages the United States has sustained because of Defendant's actions, plus a civil penalty of any amount within the applicable statutory ranges, for each violation**;**

(b) That Relator be awarded an amount that the Court decides is reasonable for recovering the proceeds of the action, including but not necessarily limited to the civil penalties and damages, on behalf of the United States, which, pursuant to the False Claims Act, shall be at least 15 percent but not more than 25 percent of the proceeds of the action or settlement of the claim if the Government intervenes and proceeds with the action, and not less than 25 percent nor more than 30 percent of the proceeds of the action or settlement of the claim if the Government does not intervene;

(c) That Relator receives all relief necessary to make Relator whole for Defendant's violations of 31 U.S.C. § 3730(h);

(d) That the Court order Defendant to award Relator front pay in lieu of reinstatement;

(e) That Relator receives an award of two times back pay, including the value of lost benefits and equity;

(f) That Relator receives an award of compensatory damages in an amount to be proven at trial for the economic, reputational, and emotional harm Relator experienced as a result of Defendant's unlawful conduct, and all other remedies and recompense allowable under 31 U.S.C. § 3730(h);

(g) That judgment be entered against Defendant in an amount to be determined at trial; and

(h) That Relator be awarded all costs and expenses incurred, including reasonable attorneys' fees; and

(i) That the Court order such other relief as is appropriate.

Trial by jury is hereby requested.

Dated: September 8, 2023

Respectfully submitted,

Plaintiff,
By her attorneys,

**/s/ Renée Brooker**
**Renée Brooker**
D.C. Bar No. 430159
**Eva U. Gunasekera**
D.C. Bar No. 502542
p*ro hac vice* to follow unsealing
Tycko & Zavareei LLP
2000 Pennsylvania Avenue NW
Suite 1010
Washington, DC 20006
(202) 417-3664
(202) 973-0950 (fax)
reneebrooker@tzlegal.com

**DO NOT SERVE**

**FALSE CLAIMS ACT COMPLAINT FILED UNDER SEAL**