

Regulation List

Part I. European Union Instruments

1. Regulation (EU) 2017/745 — Medical Device Regulation (MDR)

Official citation. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (OJ L 117, 5.5.2017, p. 1). Consolidated version in force; ELI: <http://data.europa.eu/eli/reg/2017/745/oj>

Official source. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745>

2. Regulation (EU) 2024/1689 — Artificial Intelligence (AI) Act

Official citation. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024). ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>

Official source. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

3. Regulation (EU) 2026/1744 — Digital Omnibus on AI

Official citation. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonized rules on artificial intelligence (Digital Omnibus on AI). Published OJ 24 July 2026; entered into force 27 July 2026. ELI: <http://data.europa.eu/eli/reg/2026/1744/oj>

Official source. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1744>

4. Directive (EU) 2024/2853 — Revised Product Liability Directive

Official citation. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (OJ L, 2024/2853, 18.11.2024). ELI: <http://data.europa.eu/eli/dir/2024/2853/oj>. Member States must transpose by 9 December 2026. Applies to products placed on the market or put into service after 8/9 December 2026 (see corrigendum).

Official source. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L2853>

5. Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR) Art. 9

Official citation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal

data (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). ELI:
<http://data.europa.eu/eli/reg/2016/679/oj>

Official source. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

6. Directive (EU) 2022/2555 — NIS2 Directive

Official citation. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80). ELI:
<http://data.europa.eu/eli/dir/2022/2555/oj>

Official source. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

7. Regulation (EU) 2024/2847 — Cyber Resilience Act (CRA)

Official citation. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024). ELI:
<http://data.europa.eu/eli/reg/2024/2847/oj>

Official source. <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

8. Regulation (EU) 2025/327 — European Health Data Space (EHDS)

Official citation. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327). In force since 26 March 2025. Secondary-use chapter applies from 26 March 2029 (genetic, genomic, clinical-trial and cohort data from 26 March 2031, per the slides).

Official source. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0327>

9. AI Liability Directive (AILD) — Legal Proposal Withdrawn in 2025 (Never Enacted)

Official citation. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, 28 September 2022. Withdrawn by the Commission (2025 work-programme/withdrawal list). Not law.

Official source. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>

Part II. United States Federal Instruments

10. Federal Food, Drug, and Cosmetic Act § 524B (21 U.S.C. § 360n-2) - Ensuring cybersecurity devices

Official citation. Federal Food, Drug, and Cosmetic Act § 524B, added by § 3305 of the Food and Drug Omnibus Reform Act of 2022 (FDORA), Pub. L. 117-328, div. FF, title III, 29 December 2022. Codified at 21 U.S.C. § 360n-2.

Official source. <https://uscode.house.gov/view.xhtml?req=title:21%20section:360n-2>

11. Executive Order 14365 (11 Dec 2025) - National Policy Framework for Artificial Intelligence

Official citation. Executive Order 14365 of 11 December 2025, “Ensuring a National Policy Framework for Artificial Intelligence,” 90 Fed. Reg. 58499 (16 December 2025).

Official source. <https://www.federalregister.gov/documents/2025/12/16/2025-23092/ensuring-a-national-policy-framework-for-artificial-intelligence>

Part III. United States- State Instruments

12. Texas HB 149 Texas Responsible Artificial Intelligence Governance Act (TRAIGA)

Official citation. H.B. 149, 89th Texas Legislature (2025), relating to regulation of the use of artificial intelligence systems in this state; providing civil penalties. Cited by the speaker as TRAIGA (HB 149). Effective 1 January 2026 per contemporary analyses of the enrolled act.

Official source. Texas Legislature bill text: [89\(R\) HB 149 - Enrolled version - Bill Text](#)

13. Illinois HB 1806 / Public Act 104-0054 Wellness and Oversight for Psychological Resources Act

Official citation. Public Act 104-0054, 104th Illinois General Assembly (signed 1 August 2025). Enrolled as HB 1806. Effective immediately on signing.

Official source. <https://www.ilga.gov/ftp/Public%20Acts/104/104-0054.htm>

14. California AB 489 -Health Care Professions: deceptive terms or letters: artificial intelligence

Official citation. Assembly Bill No. 489, Chapter 615, approved by the Governor 11 October 2025, filed with the Secretary of State 11 October 2025. An act to add Chapter 15.5 (commencing with Section 4999.8) to Division 2 of the Business and Professions Code, relating to healing arts. The slides state both AB 489 and SB 243 are effective 1 January 2026.

Official source. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB489

15. California Senate Bill 243 (2025) - Companion chatbots

Official citation. Senate Bill 243 (Padilla), chaptered 13 October 2025, adding Chapter 22.6 (commencing with Section 22601) to Division 8 of the Business and Professions Code. The

slides state an effective date of 1 January 2026. Subsequent 2026 legislation (including “Adam’s Law,” SB 1119, signed September 2026) builds on this baseline; that later act is not cited in the slides.

Official source. <https://leginfo.legislature.ca.gov/> (search SB 243, 2025–2026)

16. Maine LD 2082 - An Act to Regulate the Use of Artificial Intelligence in Providing Certain Mental Health Services

Official citation. LD 2082, H.P. 1397, 132nd Maine Legislature, Second Regular Session. Enacted and signed 13 April 2026; chaptered as Public Law, Chapter 687. Title: An Act to Regulate the Use of Artificial Intelligence in Providing Certain Mental Health Services.

Official source.

https://www.mainelegislature.org/legis/bills/display_ps.asp?paper=HP1397&snum=132

17. Colorado SB 24-205 (repealed) and SB 26-189 (replacement)

Official citation. SB 24-205, Colorado Artificial Intelligence Act (enacted 2024; never operatively applied in its original form). Repealed and replaced by SB 26-189, signed 14 May 2026, operative 1 January 2027, concerning the use of automated decision-making technology in consequential decisions.

Official source. <https://leg.colorado.gov/bills/sb26-189>

Part IV. Other instruments

Harmonized / International Standards

International Organization for Standardization (ISO) 14971 — Medical devices — Application of risk management to medical devices. Cited as the risk-management standard the technical file must follow.

ISO 13485 — Medical devices — Quality management systems. Cited as the certified quality-system standard.

International Electrotechnical Commission (IEC) 62304 — Medical device software — Software life cycle processes.

IEC 62366-1 — Medical devices — Application of usability engineering to medical devices. These are copyrighted standards sold by ISO, IEC, and national bodies (BSI, DIN, ANSI, etc.). They are not public-domain statutes. Notified bodies assess against them because the

MDR points to the state of the art and because harmonized standards confer a presumption of conformity when listed in the Official Journal, but the standard text itself is not Union law.

EU Guidance

Medical Device Coordination Group (MDCG) 2019-16 — Guidance on cybersecurity for medical devices. “[T]he guidance notified bodies actually assess against.” MDCG documents are endorsed by the Medical Device Coordination Group. They are not legally binding and “bind nobody in court,” which is the same caveat the speaker attaches to MDCG 2025-6.

MDCG 2025-6 — published 19 June 2025. Confirms a technical documentation file and one conformity assessment via the MDR route for AI/MDSW that is also an AI Act high-risk system. MDCG documents are published on the European Commission’s medical-devices pages ([health.ec.europa.eu / medical-devices-sector / new-regulations / guidance](https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance)).

U.S. Agency Guidance and Pathways

510(k) clearance is the premarket-notification procedure in **FDORA § 510(k)**, already covered under item 10.

FDA Predetermined Change Control Plan guidance — finalized December 2024, revised August 2025. Agency guidance describing how a manufacturer may pre-specify modifications (including to machine-learning models) in the original submission.

FDA final premarket cybersecurity guidance, June 2025 — updates “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” to address § 524B documentation. Published in the Federal Register (see 90 Fed. Reg. materials around 27 June 2025).

HIPAA (Health Insurance Portability and Accountability Act of 1996) and the HIPAA Security Rule (45 C.F.R. Part 160 and Subparts A and C of Part 164) are named only as the U.S. privacy contrast to GDPR.

PRAIM (Germany), published in *Nature Medicine*, January 2025: prospective implementation study of Vara MG in the German screening programme (463,094 women; +17.6% detection; recalls unchanged). Cited legal instruments — JALBCA / Vara symposium (13 Oct 2026)

BCSC national benchmarks, *Radiology* 2023: registry data on U.S. single-reader tomosynthesis performance.

CASES
Index of Opinions

1. Pennsylvania Real Estate Investment Trust v. SPS Technologies, Inc., No. CIV. A. 94-CV-3154, 1995 WL 687003 (E.D. Pa. Nov. 20, 1995) ([Pennsylvania Real Est. Inv. Tr. v. SPS Techs., Inc., No. CIV. A. 94-CV-3154, 1995 WL 687003 \(E.D. Pa. Nov. 20, 1995\)](#))
2. In re Ambry Genetics Data Breach Litigation, 567 F. Supp. 3d 1130 (C.D. Cal. 2021) ([In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130 \(C.D. Cal. 2021\)](#)) **(ATTACHED)**
3. Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022) ([Thaler v. Vidal, 43 F.4th 1207 \(Fed. Cir. 2022\)](#)) **(ATTACHED)**
4. Yelp Inc. v. Google LLC, No. 24-CV-06101-SVK, 2026 WL 1883619 (N.D. Cal. June 30, 2026) ([Yelp Inc. v. Google LLC, No. 24-CV-06101-SVK, 2026 WL 1883619 \(N.D. Cal. June 30, 2026\)](#))
5. In re Stem, Inc. Securities Litigation, No. 23-CV-02329-MMC, 2025 WL 3675114 (N.D. Cal. Dec. 17, 2025) ([In re Stem, Inc. Sec. Litig., No. 23-CV-02329-MMC, 2025 WL 3675114 \(N.D. Cal. Dec. 17, 2025\)](#))
6. Angelilli v. Activision Blizzard, Inc., 781 F. Supp. 3d 691 (N.D. Ill. 2025) ([Angelilli v. Activision Blizzard, Inc., 781 F. Supp. 3d 691 \(N.D. Ill. 2025\)](#))
7. United States v. Google LLC, 803 F. Supp. 3d 18 (D.D.C. 2025) ([United States v. Google LLC, 803 F. Supp. 3d 18 \(D.D.C. 2025\)](#))
8. Beyer v. DraftKings, Inc., No. 25 C 1336, 2025 WL 3281680 (N.D. Ill. Nov. 25, 2025) ([Beyer v. DraftKings, Inc., No. 25 C 1336, 2025 WL 3281680 \(N.D. Ill. Nov. 25, 2025\)](#))
9. Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138 (D. Mass. 2023) ([Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138 \(D. Mass. 2023\)](#))
10. Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023) ([Twitter, Inc. v. Taamneh, 598 U.S. 471, 143 S. Ct. 1206, 215 L. Ed. 2d 444 \(2023\)](#))
11. California v. Meta Platforms, Inc. (In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation), 753 F. Supp. 3d 849 (N.D. Cal. 2024) ([In re Soc. Media Adolescent Addiction/Pers. Inj. Prods. Liab. Litig., 753 F. Supp. 3d 849 \(N.D. Cal. 2024\)](#))



KeyCite Yellow Flag

Distinguished by [In re PowerSchool Holdings, Inc. and PowerSchool Group, LLC, Customer Security Breach Litigation](#), S.D.Cal., March 25, 2026

567 F.Supp.3d 1130

United States District Court, C.D.

California, Southern Division.

IN RE: AMBRY GENETICS DATA BREACH LITIGATION

Lead Case No.: SACV 20-00791-CJC (KESx)

|

Signed 10/18/2021

Synopsis

Background: Customers filed putative class action against companies that provided genetic-testing services arising from data breach, alleging claims under California law for negligence, invasion of privacy, breach of contract, breach of implied contract, breach of fiduciary duty, and breach of confidence, for violation of the California Unfair Competition Law (UCL), the California Confidentiality of Medical Information Act (CMIA), the California Consumer Legal Remedies Act (CLRA), the California Consumer Records Act (CRA), and the Illinois Genetic Information Privacy Act (IGIPA), and for injunctive and declaratory relief. Companies moved to dismiss for failure to state a claim, and customers moved for leave to amend.

Holdings: The District Court, [Cormac J. Carney, J.](#), held that:

[1] customers adequately alleged causation, as required for Article III standing;

[2] customers adequately alleged causation, as required for negligence claim;

[3] economic loss doctrine did not bar customers' negligence claim;

[4] customers stated claim for invasion of privacy under California law;

[5] customers stated claim for unjust enrichment under California law, as construed by Ninth Circuit;

[6] customers stated claim for violation of negligent-disclosure provision of CMIA;

[7] customers stated claim for violation of the CRA as to California residents; but

[8] hackers' accessing of data did not amount to disclosure by companies in violation of the IGIPA.

Motions granted in part and denied in part.

Procedural Posture(s): Motion to Dismiss for Failure to State a Claim; Motion to Amend the Complaint.

West Headnotes (54)

[1] Corporations and Business

Organizations 🔑 Parent and subsidiary corporations

Customers of genetic-testing corporation, which had been acquired by parent corporation, could state claims against subsidiary corporation only on theory that it failed to take appropriate and necessary measures as result of due diligence after it was founded, but not on theory that it failed to engage in due diligence prior to parent corporation's acquisition of genetic-testing corporation, in action raising negligence and other claims against genetic-testing corporation and subsidiary corporation by customers whose data was accessed in data breach; subsidiary corporation was founded after parent corporation acquired genetic-testing corporation, and it would have been impossible for subsidiary corporation to participate in any due diligence before acquisition because it did not even exist.

[More cases on this issue](#)

[2] Federal Civil Procedure 🔑 In general; injury or interest

Federal Courts 🔑 Case or Controversy Requirement

To constitute an actual case or controversy under Article III, the plaintiffs bringing a case must have standing. [U.S. Const. art. 3, § 2, cl. 1.](#)

- [3] **Federal Civil Procedure** 🔑 In general; injury or interest

Federal Civil Procedure 🔑 Causation; redressability

To satisfy the standing requirement of Article III, a plaintiff must show that (1) he has suffered an injury in fact that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical, (2) the injury is fairly traceable to the defendant's challenged actions, and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *U.S. Const. art. 3, § 2, cl. 1.*

- [4] **Federal Civil Procedure** 🔑 Causation; redressability

For Article III standing to exist, there must be a causal connection between the injury and the conduct complained of; the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. *U.S. Const. art. 3, § 2, cl. 1.*

- [5] **Federal Civil Procedure** 🔑 Pleading

Although at the pleading stage allegations that the plaintiff's injury was caused by the defendant's conduct may suffice to establish the causation required for Article III standing, those allegations must be supported by facts, not merely legal conclusions. *U.S. Const. art. 3, § 2, cl. 1.*

- [6] **Telecommunications** 🔑 Persons entitled to sue, standing, and parties

Customers adequately alleged that their injuries from information stolen in data breach were caused by breach of genetic-testing companies' information systems in phishing incident, as required to establish Article III standing at pleading stage to bring claims for negligence and other causes of action arising from breach;

customers alleged that information exposed in breach included their names, dates of birth, Social Security numbers, medical information, and other personal information, and that they suffered injuries including receiving suspicious communications relating to their banking, credit, and password-related information, having to contact banks, credit card agencies, and credit bureaus, and having to monitor their bank accounts and credit. *U.S. Const. art. 3, § 2, cl. 1.*

[4 Cases that cite this headnote](#)

[More cases on this issue](#)

- [7] **Telecommunications** 🔑 Unauthorized access to or transmission of electronic communications; electronic surveillance

Customers adequately alleged that data breach was sufficiently likely to recur, such that injunctive relief requiring genetic-testing companies to implement particular security measures would redress customers' injuries from theft of personal information, as required to establish Article III standing at pleading stage to seek injunctive relief in action raising negligence and other claims; customers asserted that requested measures were necessary because companies still possessed their private information, that companies had announced few, if any, changes to data-security infrastructure and procedures to fix vulnerabilities, and that companies' insufficient data security was known to hackers, rendering their private information more vulnerable. *U.S. Const. art. 3, § 2, cl. 1.*

[6 Cases that cite this headnote](#)

[More cases on this issue](#)

- [8] **Federal Civil Procedure** 🔑 Causation; redressability

To show redressability, as required for Article III standing, plaintiffs must show that it is likely, as opposed to merely speculative, that their injury will be redressed by a favorable decision. *U.S. Const. art. 3, § 2, cl. 1.*

[9] Federal Civil Procedure 🔑 In general; injury or interest

Plaintiffs must demonstrate Article III standing separately for each form of relief sought. *U.S. Const. art. 3, § 2, cl. 1.*

[10] Injunction 🔑 Persons entitled to apply; standing

To demonstrate Article III standing to pursue prospective injunctive relief, plaintiffs must demonstrate a concrete injury and a realistic likelihood that the injury will be repeated. *U.S. Const. art. 3, § 2, cl. 1.*

[2 Cases that cite this headnote](#)

[11] Negligence 🔑 Elements in general

The elements of a negligence claim under California law are duty, breach, causation, and injury.

[6 Cases that cite this headnote](#)

[12] Negligence 🔑 Substantial factor

To demonstrate actual or legal causation, as an element of negligence under California law, the plaintiff must show that the defendant's act or omission was a substantial factor in bringing about the injury.

[2 Cases that cite this headnote](#)

[13] Negligence 🔑 Miscellaneous particular cases

Customers adequately alleged causation between data breach and their alleged damages from theft of personal information, as required to state claim for negligence under California law against genetic-testing companies whose information systems were breached in phishing incident; customers alleged that information exposed in breach included their names, dates of birth, Social Security numbers, medical information, and other personal information, and that they suffered injuries including receiving suspicious communications relating to their banking, credit, and password-related

information, having to contact banks, credit card agencies, and credit bureaus, and having to monitor their bank accounts and credit.

[2 Cases that cite this headnote](#)

[14] Negligence 🔑 Miscellaneous particular cases

Customers adequately alleged that genetic-testing companies were negligent by waiting three months to notify them of data breach and failing to notify them sooner, as required for causation element of negligence claim under California law; customers alleged that delay in notification prevented them from taking appropriate protective measures that could have prevented some of the damages they suffered, such that they suffered incrementally increased damages that they would not have suffered with timely notice, and some customers alleged that they suffered injuries from breach before they were notified of it that they might have been able to take steps to avoid had they been notified sooner.

[15] Negligence 🔑 Economic loss doctrine

Customers whose personal information was stolen in data breach did not allege merely economic injury, and thus economic loss doctrine did not bar their negligence claims under California law against genetic-testing companies whose information systems were hacked in phishing incident; customers alleged privacy injury stemming from unauthorized sharing of their private medical information, customers further alleged injuries such as anxiety, concern, and unease, and customers alleged that they spent many hours responding to the data breach.

[13 Cases that cite this headnote](#)

[16] Torts 🔑 Economic loss doctrine

Under California's "economic loss doctrine," purely economic losses are not recoverable in tort.

[7 Cases that cite this headnote](#)

[More cases on this issue](#)

[17] Negligence 🔑 [Economic loss doctrine](#)

Under California law, in the absence of personal injury, physical damage to property, a special relationship between the parties, or some other common law exception to the economic loss doctrine, recovery of purely economic loss for negligence is foreclosed.

[8 Cases that cite this headnote](#)

[18] Negligence 🔑 [Violations of statutes and other regulations](#)

Under California law, negligence per se is not separate cause of action, but rather evidentiary presumption that party failed to exercise due care in certain limited circumstances.

[3 Cases that cite this headnote](#)

[19] Negligence 🔑 [Violations of statutes and other regulations](#)

Customers' reliance on genetic-testing companies' alleged violations of FTC Act prohibiting unfair practices in or affecting commerce and Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy laws did not bar their negligence claims based on California's negligence per se doctrine on ground that FTC Act and HIPAA did not provide private right of action, in action arising from data breach resulting in theft of customers' personal information; customers were not attempting to sue under FTC Act or HIPAA, but rather were relying on statutes to establish that companies failed to exercise due care, as part of their negligence action. Federal Trade Commission Act, § 1 et seq., [15 U.S.C.A. § 41 et seq.](#)

[4 Cases that cite this headnote](#)

[20] Negligence 🔑 [Violations of statutes and other regulations](#)

Negligence 🔑 [Violations of statutes and other regulations](#)

On a claim of negligence per se under California law, plaintiffs asserting that defendants have violated statutes are not attempting to sue under

the statutes, but rather the statutes serve the subsidiary function of providing evidence of an element of a preexisting common-law cause of action.

[1 Case that cites this headnote](#)

[21] Negligence 🔑 [Violations of statutes and other regulations](#)

On a claim of negligence per se under California law, it is the tort of negligence, and not the violation of the statute itself, which entitles a plaintiff to recover civil damages; the plaintiff is not attempting to pursue a private cause of action for violation of the statute, but rather he is pursuing a negligence action and is relying upon the violation of a statute, ordinance, or regulation to establish part of that cause of action.

[7 Cases that cite this headnote](#)

[22] Torts 🔑 [Intrusion](#)

To state a claim for invasion of privacy under California law, plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is so serious as to constitute an egregious breach of the social norms such that the breach is highly offensive.

[16 Cases that cite this headnote](#)

[23] Torts 🔑 [Intrusion](#)

Determining whether a defendant's actions were highly offensive to a reasonable person, as element of invasion of privacy under California law, requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.

[5 Cases that cite this headnote](#)

[24] Constitutional Law 🔑 [Telecommunications](#)
Torts 🔑 [Particular cases in general](#)

Customers whose personal information, including medical information, was stolen in data breach of genetic-testing companies' information systems adequately alleged invasion of privacy claim under California law, where customers alleged that companies knew their information-security practices were inadequate and had numerous security vulnerabilities, that companies intentionally, willfully, recklessly, or negligently failed to take adequate and reasonable measures to ensure their data systems were protected, that companies knew their inadequate data-security measures would likely result in a breach, and that companies knew that such a breach would harm customers.

[10 Cases that cite this headnote](#)

[25] Telecommunications 🔑 **Breach of contract**

Customers failed to allege existence of promises by genetic-testing companies to keep customers' personal information safe, and thus they failed to state a claim for breach of express contract under California law arising from data breach in which information was stolen by hackers in phishing incident; alleged contract terms merely contained broad statements regarding commitment to protecting privacy, caring about data, method of encryption of data, and maintenance of confidentiality in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) and applicable state law.

[More cases on this issue](#)

[26] Contracts 🔑 **Pleading contract or specifications**

A claim for breach of contract under California law must allege the specific provisions in the contract creating the obligation the defendant is said to have breached.

[2 Cases that cite this headnote](#)

[27] Telecommunications 🔑 **Breach of contract**

Customers of genetic-testing companies whose information was stolen by hackers in data

breach stated claim against companies for breach of implied contract under California law, where they alleged that they gave their private information to companies for purposes of obtaining genetic testing with the understanding that companies would take adequate measures to protect the information, and mandatory receipt of Social Security numbers and other sensitive personal information implied recipient's intent to sufficiently protect information.

[6 Cases that cite this headnote](#)

[More cases on this issue](#)

[28] Contracts 🔑 **Implied agreements**

Under California law, an implied-in-fact contract requires proof of the same elements necessary to evidence an express contract: mutual assent or offer and acceptance, consideration, legal capacity, and lawful subject matter.

[3 Cases that cite this headnote](#)

[29] Contracts 🔑 **Implied agreements**

Under California law, an implied contract requires that both parties agree to its terms and have a meeting of the minds, but the creation of an implied contract can be manifested by conduct rather than words.

[2 Cases that cite this headnote](#)

[30] Unjust Enrichment and Constructive

Contracts 🔑 **Elements of unjust enrichment in general**

To allege unjust enrichment as an independent cause of action under California law, as construed by the Ninth Circuit, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff's expense.

[3 Cases that cite this headnote](#)

[31] Unjust Enrichment and Constructive

Contracts 🔑 **Particular Cases and Contexts**

Customers whose personal information was stolen during data breach stated claim for unjust enrichment under California law, as construed by

Ninth Circuit, against genetic-testing companies; customers alleged that they paid companies money for genetic-testing services, that they expected that a portion of their payments would go toward data management and security, and that companies retained that benefit despite not having implemented adequate safeguards for customers' private information.

[7 Cases that cite this headnote](#)

[More cases on this issue](#)

[32] Fraud 🔑 [Fiduciary or confidential relations](#)

Allegations that genetic-testing companies collected customers' private information, which customers entrusted to them, so that companies could provide their genetic testing to screen for and diagnose diseases, did not establish fiduciary relationship between customers and companies under California law, and thus companies were not liable for breach of fiduciary duty arising from data breach in which customers' information, including their dates of birth, Social Security numbers, and medical information was stolen by hackers; companies never agreed to subordinate their interests to customers' interests, and customers were not so vulnerable as to give rise to equitable concerns, but rather they merely entered into arms-length transaction.

[1 Case that cites this headnote](#)

[More cases on this issue](#)

[33] Fraud 🔑 [Fiduciary or confidential relations](#)

Under California law, a “fiduciary relationship” is any relation existing between parties to a transaction wherein one of the parties is duty bound to act with the utmost good faith for the benefit of the other party.

[3 Cases that cite this headnote](#)

[34] Fraud 🔑 [Fiduciary or confidential relations](#)

Traditional examples of fiduciary relationships under California law include those of trustee/beneficiary, corporate directors and majority shareholders, business partners, joint adventurers, and agent/principal; inherent in

each of these relationships is the duty of undivided loyalty the fiduciary owes to its beneficiary, imposing on the fiduciary obligations far more stringent than those required of ordinary contractors.

[35] Torts 🔑 [Miscellaneous torts in general](#)

Tort for breach of confidence under California law is based upon concept of implied obligation or contract between parties that confidential information will not be disclosed.

[1 Case that cites this headnote](#)

[36] Torts 🔑 [Miscellaneous torts in general](#)

To sufficiently allege a breach of confidence claim under California law, a plaintiff must allege that (1) the plaintiff conveyed confidential and novel information to the defendant; (2) the defendant had knowledge that the information was being disclosed in confidence; (3) there was an understanding between the defendant and the plaintiff that the confidence be maintained; and (4) there was a disclosure or use in violation of the understanding.

[6 Cases that cite this headnote](#)

[37] Torts 🔑 [Miscellaneous torts in general](#)

Unauthorized parties' accessing of email account of employee of genetic-testing companies to acquire customers' confidential information was not disclosure of customers' information by companies, as required to support cause of action for breach of confidence under California law, absent indication that companies affirmatively shared any information or performed any act that gave information to hackers.

[4 Cases that cite this headnote](#)

[38] Antitrust and Trade

Regulation 🔑 [Injunction](#)

Antitrust and Trade

Regulation 🔑 [Monetary Relief; Damages](#)

Remedies under California's Unfair Competition Law (UCL) are limited to restitution and injunctive relief, and do not include damages. [Cal. Bus. & Prof. Code § 17200](#).

[4 Cases that cite this headnote](#)

[39] Antitrust and Trade Regulation [Injunction](#)

Antitrust and Trade

Regulation [Monetary Relief; Damages](#)

Restitution and injunctive relief are equitable remedies, and thus are not available under California's Unfair Competition Law (UCL) unless plaintiff lacks adequate remedy at law. [Cal. Bus. & Prof. Code § 17200](#).

[4 Cases that cite this headnote](#)

[40] Antitrust and Trade Regulation [Monetary Relief; Damages](#)

Plaintiff must establish that she lacks adequate remedy at law before securing equitable restitution for past harm under California's Unfair Competition Law (UCL). [Cal. Bus. & Prof. Code § 17200](#).

[3 Cases that cite this headnote](#)

[41] Antitrust and Trade Regulation [Injunction](#)

Antitrust and Trade

Regulation [Monetary Relief; Damages](#)

Customers failed to allege that legal remedies they sought for injuries they incurred as result of genetic-testing companies' past failure to protect their private information, which was stolen by hackers in data breach, were inadequate, and thus customers were not entitled to restitution or injunctive relief under California's Unfair Competition Law (UCL); customers' claim was based on allegation that companies failed to take adequate measures to protect their private information, not any allegation that companies were failing to prevent future data breaches, and throughout their complaint, which raised negligence and other claims, customers sought

compensatory damages for past harm. [Cal. Bus. & Prof. Code § 17200](#).

[More cases on this issue](#)

[42] Health [Confidentiality; patient records](#)

Hackers' unauthorized accessing of email account belonging to employee of genetic-testing companies to steal customers' confidential information was not disclosure of customers' information by companies, as required to support cause of action under California's Confidentiality of Medical Information Act (CMIA) prohibiting unauthorized disclosure of medical information, absent indication that companies performed any affirmative communicative act that gave hackers information. [Cal. Civ. Code § 56.10](#).

[2 Cases that cite this headnote](#)

[43] Health [Confidentiality; patient records](#)

"Disclosure," under California's Confidentiality of Medical Information Act (CMIA) prohibiting unauthorized disclosure of medical information, refers to affirmative communicative acts—giving out medical information on a patient. [Cal. Civ. Code § 56.10](#).

[3 Cases that cite this headnote](#)

[44] Health [Confidentiality; patient records](#)

In contrast to disclosure under section of California's Confidentiality of Medical Information Act (CMIA) prohibiting unauthorized disclosure of medical information, section prohibiting negligent release of medical information does not require an affirmative communicative act but instead can be accomplished by negligently allowing information to end up in the possession of an unauthorized person. [Cal. Civ. Code § 56.101](#).

[2 Cases that cite this headnote](#)

[45] Health [Confidentiality; patient records](#)

A plaintiff bringing an action for negligent release of confidential information

under California's Confidentiality of Medical Information Act (CMIA) must allege that a defendant's negligence resulted in unauthorized or wrongful access to the information, i.e., that the information was improperly viewed or otherwise accessed. [Cal. Civ. Code § 56.101](#).

[3 Cases that cite this headnote](#)

[46] Health 🔑 Confidentiality; patient records

Customers sufficiently alleged that their information was viewed by third parties, as required to state claim against genetic-testing companies for negligent release of confidential information under California's Confidentiality of Medical Information Act (CMIA) arising from data breach, where customers alleged that unauthorized parties had accessed and viewed their unencrypted, unredacted information, including relevant medical records. [Cal. Civ. Code § 56.101](#).

[1 Case that cites this headnote](#)

[47] Antitrust and Trade Regulation 🔑 Monetary Relief; Damages

Customers failed to establish that legal remedies they sought to address genetic-testing companies' past conduct that resulted in data breach were inadequate, and thus customers were not entitled to equitable restitution under California's Consumer Legal Remedies Act (CLRA) for companies' alleged conduct in representing that they had taken appropriate measures to protect customers' private information but then failing to protect that information. [Cal. Civ. Code § 1770\(a\)\(5\)](#).

[More cases on this issue](#)

[48] Antitrust and Trade Regulation 🔑 Privacy

Customers adequately alleged that genetic-testing companies' approximately three-month delay in notifying them of data breach was unreasonable, as required to state claim for violation of California's Consumer Records Act (CRA); customers alleged that companies' delay prevented them from taking appropriate

protective measures that could have prevented some of the damages they suffered, and that they suffered injuries resulting from breach before they were notified of it that they might have been able to take steps to avoid had they been notified sooner, such that companies' delay caused them to incur more damages than they would have incurred with timely notice. [Cal. Civ. Code § 1798.82](#).

[2 Cases that cite this headnote](#)

[49] Antitrust and Trade Regulation 🔑 Private entities or individuals

Federal Civil Procedure 🔑 Consumers, purchasers, borrowers, and debtors

Customers whose personal information was accessed by hackers in data breach could assert claims under California's Consumer Records Act only on behalf of California residents, in putative class action against genetic-testing companies. [Cal. Civ. Code § 1798.82](#).

[2 Cases that cite this headnote](#)

[50] Health 🔑 Confidentiality; patient records

Hackers' unauthorized access of email account belonging to employee of genetic-testing companies to steal customers' confidential information was not disclosure by companies, as required for liability under provision of the Illinois Genetic Information Privacy Act (IGIPA) prohibiting use or disclosure of genetic-related information except in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA), or provision prohibiting disclosure in manner that permitted identification of subject of genetic tests, absent indication that companies affirmatively shared information or performed any act that gave hackers information. [410 Ill. Comp. Stat. Ann. 513/30, 513/31.10](#).

[2 Cases that cite this headnote](#)

[51] Health 🔑 Confidentiality; patient records

Customers whose information was subject of data breach sufficiently alleged harm stemming

from disclosure of their genetic information, as required to state claim against genetic-testing companies for violation of provision of Illinois Genetic Information Privacy Act (IGIPA) governing to whom genetic testing and information derived from genetic testing could be released, where customers alleged harm to their privacy interests from disclosure of the information. 410 Ill. Comp. Stat. Ann. 513/15.

[1 Case that cites this headnote](#)

[52] Health 🔑 Confidentiality; patient records

Customers plausibly alleged that information derived from genetic testing was released in data breach, as required to state claim against genetic-testing companies for violation of provision of Illinois Genetic Information Privacy Act (IGIPA) governing to whom genetic testing and information derived from genetic testing could be released, where customers alleged that their medical information and diagnosis information was released in breach. 410 Ill. Comp. Stat. Ann. 513/15.

[1 Case that cites this headnote](#)

[53] Federal Civil Procedure 🔑 Pleading over

Customers whose personal information was subject of data breach were not entitled to leave to amend complaint to replead claims against genetic-testing companies, including claims for breach of express contract, breach of fiduciary duty, breach of confidence, violation of provision of California Confidentiality of Medical Information Act (CMIA), and violation of the California Consumer Records Act (CRA) as to non-California residents, on grant of motion to dismiss for failure to state a claim; motion was companies' fourth motion to dismiss customers' complaints, each motion generally raised same issues, customers had failed to cure deficiencies despite multiple opportunities to do so, and there was no indication that they could allege new facts that would plausibly state claims. Cal. Civ. Code §§ 56.10, 1798.82; Fed. R. Civ. P. 15(a).

[More cases on this issue](#)

[54] Federal Civil Procedure 🔑 Pleading over

Customers whose personal information was subject of data breach were entitled to leave to amend complaint to replead claims against genetic-testing companies for violation of the California Unfair Competition Law (UCL) and Consumer Legal Remedies Act (CLRA), on grant of companies' fourth motion to dismiss for failure to state a claim, where companies' argument that customers failed to allege the legal remedies they sought to redress past conduct were inadequate was raised for first time in current motion. Cal. Bus. & Prof. Code § 17200; Cal. Civ. Code § 1770(a)(5).

[More cases on this issue](#)

***1138 ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS PLAINTIFFS' SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT [Dkt. 95]**

CORMAC J. CARNEY, UNITED STATES DISTRICT JUDGE

I. INTRODUCTION

In this consolidated putative class action, Plaintiffs from 15 different states allege 13 claims against Defendants Ambry Genetics Corporation (“Ambry”) and Konica Minolta Precision Medicine, Inc. (“KMPM”) arising out of a 2020 data breach. (Dkt. 90 [Unredacted Second Amended Consolidated Class Action Complaint, hereinafter “SAC”].) Before the Court is Defendants’ motion to dismiss the SAC. (Dkt. 95 [hereinafter “Mot.”]). For the following reasons, Defendants’ motion is **GRANTED IN PART AND DENIED IN PART**.

II. BACKGROUND

Ambry provides genetic testing that screens and diagnoses medical issues including [hereditary cancer](#), hereditary [cardiovascular disease](#), neurodevelopmental disorders, and [epilepsy](#). (SAC ¶¶ 1, 45.) Between January 22 and 24, 2020, it experienced a data breach involving [names](#), dates of birth, Ambry account numbers, health insurance information, confidential medical information, medical diagnoses, billing

information including addresses, email addresses, and telephone numbers, and Social Security numbers. (*Id.* ¶¶ 2–3, 13, 24–48, 67, 71, 76); *see also* Ambry Genetics Substitute Notice, *available at* <https://www.ambrygen.com/legal/substitute-notice>. Specifically, hackers accessed through a phishing incident the email account of an Ambry employee for multiple days, giving the hackers access to about 233,000 customers’ information. (SAC ¶¶ 66–67.) Plaintiffs allege that “[t]he Data Breach was a direct result of Defendants’ failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients’ Private Information.” (*Id.* ¶ 17.) Nearly 3 months later, on April 15, 2020, Ambry sent a Notice of Data Breach to the affected customers. (*Id.* ¶ 73.)

Plaintiffs allege claims for (1) negligence, (2) invasion of privacy, (3) breach of ***1139** contract, (4) breach of implied contract, (5) unjust enrichment, (6) breach of fiduciary duty, (7) breach of confidence, (8) violation of the California Unfair Competition Law (the “UCL,” [Cal. Business & Professions Code § 17200, et seq.](#)), (9) violation of the California Confidentiality of Medical Information Act (the “CMIA,” [Cal. Civ. Code § 56, et seq.](#)), (10) violation of the California Consumer Legal Remedies Act (the “CLRA,” [Cal. Civ. Code § 1750, et seq.](#)), (11) violation of the California Consumer Records Act (the “CRA,” [Cal. Civ. Code § 1798.82 et seq.](#)), (12) violation of the Illinois Genetic Information Privacy Act (the “IGIPA,” 410 ILCS 513), and (13) injunctive and declaratory relief. (*Id.* ¶ 21.)

Plaintiffs seek to represent the following classes: (1) a nationwide class, (2) a nationwide adult sub-class, (3) a nationwide minor sub-class, (4) an Arizona subclass, (5) a California sub-class, (6) a Florida sub-class, (7) a Georgia sub-class, (8) an Illinois sub-class, (9) an Indiana sub-class, (10) a Michigan sub-class, (11) a Minnesota sub-class, (12) a New Jersey sub-class, (13) a New York sub-class, (14) an Ohio sub-class, (15) a Pennsylvania sub-class, (16) a Tennessee sub-class, (17) a Virginia sub-class, and (18) a West Virginia sub-class. (*Id.* ¶¶ 376–78.)

III. ANALYSIS

Defendants argue that KMPM is not properly named as a defendant in this action and that Plaintiffs lack standing. Defendants further move to dismiss each of Plaintiffs’ 13 claims for reasons described below. The Court addresses each of Defendants’ arguments in turn.

A. KMPM

KMPM argues that it is not properly named as a defendant in this case. (Mot. at 6–8.) Plaintiffs allege that “KMPM was founded in 2018 after Konica Minolta, Inc. acquired Ambry in 2017 for up to \$1 billion.” (SAC ¶ 50.) Plaintiffs further allege that “KMPM either failed to engage in ... due diligence [prior to Ambry’s acquisition] or failed to take appropriate and necessary measures as a result of the due diligence that would have protected the Private Information of Plaintiffs and Class Members.” (*Id.* ¶ 56.) However, according to Plaintiffs’ allegations, it would have been impossible for KMPM to participate in any due diligence before the acquisition because KMPM did not even exist. (*See id.* ¶ 50.) Plaintiffs therefore cannot state a claim for relief against KMPM on the theory that it failed to engage in due diligence. They can only state a claim for relief against KMPM on the theory that it failed to take appropriate and necessary measures in response to due diligence after it was founded.

B. Standing

[1] [2] [3] Defendants next argue that Plaintiffs lack standing to pursue their claims. [Article III of the United States Constitution](#) requires that courts adjudicate only actual cases or controversies. To constitute an actual case or controversy, the plaintiffs bringing a case must have standing. The party invoking federal jurisdiction bears the burden of establishing standing. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992). To satisfy the standing requirement, a plaintiff must show that (1) he has suffered an injury in fact that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical, (2) the injury is fairly traceable to the defendant’s challenged actions, and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. ***1140** *Friends of the Earth, Inc. v. Laidlaw Env’t Servs., Inc.*, 528 U.S. 167, 180–81, 120 S.Ct. 693, 145 L.Ed.2d 610 (2000). Defendants do not argue that Plaintiffs have failed to state a concrete and particularized and actual or imminent injury. Rather, they argue that (1) Plaintiffs’ alleged injury is not fairly traceable to Defendants’ challenged actions, and (2) that it is not likely that Plaintiffs’ injury will be redressed by the injunctive relief they seek. (Mot. at 9–14.)

1. Causation

[4] [5] For [Article III](#) standing to exist, “there must be a causal connection between the injury and the conduct

complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.” *Lujan*, 504 U.S. at 560, 112 S.Ct. 2130 (cleaned up). Although at the pleading stage, allegations that the plaintiff’s injury was caused by the defendant’s conduct may suffice, those allegations must be supported by facts, not merely legal conclusions. *Id.* at 561, 112 S.Ct. 2130; *Ashcroft v. Iqbal*, 556 U.S. 662, 679, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009).

[6] Defendants argue that Plaintiffs fail to plausibly allege that their injuries were caused by Defendants’ actions. The Court disagrees. Plaintiffs allege that the information exposed in the data breach includes their names, dates of birth, Ambry account numbers, health insurance information, confidential medical information, medical diagnoses, billing information including addresses, email addresses, and telephone numbers, and Social Security numbers. (SAC ¶¶ 2–3, 13, 24–48, 67, 71, 76.) Plaintiffs allege that they suffered injuries including receiving suspicious telephone calls, emails, and text messages (SAC ¶¶ 116 [Annoni], 130 [Brodsky], 142 [Coleman], 156 [Domingues], 162 [Ferrier], 186 [Jasielum], 213 [Nakagoshi], 227 [O’Hara], 255 [Taglioli], 269 [Velardi]), notifications that a bank conducted a hard inquiry on their credit without authorization (*id.* ¶ 254 [Taglioli]), notifications that someone attempted to pass bad checks through use of their identity and other fraudulent bank activity (*id.* ¶¶ 191 [Kanawati], 222 [Neumann]), notifications that an unauthorized party obtained their passwords (*id.* ¶¶ 156 [Domingues], 192 [Kanawati]), and notifications that they were logged into their accounts from new, unrecognized devices (*id.* ¶ 220 [Neumann]). They further allege that they had to contact banks, credit card agencies, and credit bureaus to cancel credit or debit cards and monitor checking accounts and credit, (*id.* ¶¶ 122 [Barduca], 134 [Cercas], 139 [Coleman], 146 [Cooperson], 153 [Domingues], 183 [Jasielum], 190 [Kanawati], 198 [McMurphy], 246 [Stewart]), and contact insurance companies to alert them of the breach and request new account numbers (*id.* ¶¶ 134 [Cercas], 183 [Jasielum]). Unlike in past iterations of the SAC, (*see* Dkt. 68 [Order Granting Defendants’ Motion to Dismiss Plaintiffs’ First Amended Consolidated Complaint]), Plaintiffs sufficiently connect the information stolen and the alleged injuries to establish standing at the pleading stage.

2. Redressability as to Injunctive Relief

[7] [8] [9] [10] Defendants next argue that Plaintiffs cannot show that the injunctive relief they seek will redress Plaintiffs’ injury stemming from a previous data breach. (Mot. at 13–14.) To show redressability, Plaintiffs must show that it is likely, as opposed to merely speculative, that their injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180–81, 120 S.Ct. 693, 145 L.Ed.2d 610 (2000). They “must demonstrate standing separately for each form *1141 of relief sought.” *Id.* at 185, 120 S.Ct. 693. “To demonstrate standing to pursue prospective injunctive relief, plaintiffs must demonstrate a concrete injury and a realistic likelihood that the injury will be repeated.” *Taylor v. Westly*, 488 F.3d 1197, 1199 (9th Cir. 2007).

Plaintiffs seek injunctive relief requiring Defendants to “implement and maintain reasonable security measures,” including ordering that Defendants hire security auditors, audit and train their security personnel, segment patient data through firewalls and access controls, and other measures. (SAC ¶ 566.) They allege that these measures are necessary because Defendants still possess their private information and “Defendants have announced few if any changes to [their] data security infrastructure, processes or procedures to fix the vulnerabilities in [their] computer systems and/or security practices which permitted the Data Breach to occur.” (*Id.* ¶¶ 561–62.) Plaintiffs further allege that “now that Defendants’ insufficient data security is known to hackers, the Private Information in Defendants’ possession is even more vulnerable to cyberattack.” (*Id.* ¶ 563.) At the pleading stage, these allegations are sufficient to allege that a data breach is sufficiently likely to recur such that injunctive relief will redress Plaintiffs’ injuries.

C. Negligence

Defendants move to dismiss Plaintiffs’ negligence claim on the bases that (1) Plaintiffs fail to allege causation and (2) the economic loss doctrine bars the claim. Defendants also argue that Plaintiffs should not be able to rely on the negligence *per se* doctrine.

1. Causation

[11] [12] The elements of a negligence claim under California law are duty, breach, causation, and injury. *Vasilenko v. Grace Family Church*, 3 Cal. 5th 1077, 1083, 224 Cal.Rptr.3d 846, 404 P.3d 1196 (2017). “[T]o demonstrate

actual or legal causation, the plaintiff must show that the defendant's act or omission was a 'substantial factor' in bringing about the injury." *Saelzler v. Advanced Group 400*, 25 Cal. 4th 763, 774, 107 Cal.Rptr.2d 617, 23 P.3d 1143 (2001).

Plaintiffs allege that Defendants were negligent by (1) failing to take steps to prevent a data breach (SAC ¶¶ 398–411), and (2) waiting 3 months to notify Plaintiffs of the breach (*id.* ¶¶ 3, 5, 70–71, 366, 408). Defendants argue that Plaintiffs' negligence claim must be dismissed on both theories because Plaintiffs have failed to show causation between the data breach and Plaintiffs' alleged damages. (Mot. at 14.)

[13] [14] As to the first theory, as explained in Section III.B.1., Plaintiffs have sufficiently demonstrated causation between the data breach and Plaintiffs' alleged damages. As to the second theory, Plaintiffs have also sufficiently demonstrated causation between the delayed notification and Plaintiffs' increased damages. Specifically, Plaintiffs allege that the delay prevented them from taking appropriate protective measures that could have prevented some of the damages they suffered, and they therefore suffered "incrementally increased damages" that they would not have suffered with timely notice. (SAC ¶¶ 544–45.) Indeed, some Plaintiffs allege that they suffered injuries resulting from the breach before they were notified of it that they might have been able to take steps to avoid had they been notified sooner. (See, e.g., *id.* ¶¶ 142 [Coleman receiving fraudulent phone call from someone attempting to get money on March 5, 2020], 263 [Terrano being denied credit limit increase in March 2020].) These allegations *1142 are sufficient to state a claim that Defendants were negligent by failing to notify Plaintiffs of the data breach sooner.

2. Economic Loss Doctrine

[15] [16] [17] Defendants also argue that Plaintiffs' negligence claim is barred by the economic loss doctrine. Under the economic loss doctrine, "purely economic losses are not recoverable in tort." *NuCal Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) (citation omitted). In the absence of personal injury, physical damage to property, a special relationship between the parties, or some other common law exception to the rule, recovery of purely economic loss for negligence is foreclosed. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 803–04, 157 Cal.Rptr. 407, 598 P.2d 60 (1979).

However, Plaintiffs have not alleged merely economic injury. Rather, they have alleged a privacy injury stemming from the unauthorized sharing of their private medical information. (See SAC ¶¶ 119, 124, 129, 136, 141, 148, 155, 161, 168, 175, 180, 185, 195, 200, 205, 212, 219, 229, 234, 241, 248, 253, 261, 268, 275, 419–421.) They have further alleged injuries such as anxiety, concern, and unease. (*Id.* ¶¶ 118, 128, 135, 147, 154, 160, 167, 204, 218, 247, 267, 274.) And they have alleged that they spent many hours responding to the data breach. (See, e.g., *id.* ¶¶ 115, 122, 127, 134, 139, 146, 153, 159, 166, 183, 190, 198, 203, 210); see also *Stasi v. Immediata Health Grp. Corp.*, 501 F.Supp.3d 898, 913 (S.D. Cal. 2020) ("[T]ime spent responding to a data breach is a non-economic injury, that when alleged to support a negligence claim, defeats an economic loss doctrine argument.") (citing *In re Solara Medical Supplies, LLC Customer Data Security Breach Litig.*, — F.Supp.3d —, —, 2020 WL 2214152, at *4 (S.D. Cal. 2020) (involving theft of medical information); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) (involving the hack of non-financial personal information)). Accepting their allegations as true and construing them in their favor, Plaintiffs have sufficiently alleged a claim for negligence.

3. Negligence Per Se

[18] Under California law, "negligence per se is not a separate cause of action, but rather an evidentiary presumption that a party failed to exercise due care in certain limited circumstances." *Ward v. Litton Loan Servicing, LP*, 2012 WL 13024081, at *5 (C.D. Cal. Apr. 10, 2012). Plaintiffs allege that Defendants were negligent in their handling of Plaintiffs' private information. In support of their contention that Defendants failed to exercise due care, they allege that Defendants violated Section 5 of the FTC Act, which prohibits "unfair ... practices in or affecting commerce," as well as HIPAA privacy laws. (SAC ¶¶ 413, 418–19.)

[19] [20] [21] Defendants argue that Plaintiffs' reliance on the doctrine of negligence *per se* fails because the FTC Act and HIPAA do not provide a private right of action. (Mot. at 18.) But Plaintiffs are not attempting to sue under these statutes. Rather, the statutes "instead serve[] the subsidiary function of providing evidence of an element of a pre-existing common law cause of action." *Crusader Ins. Co. v. Scottsdale Ins. Co.*, 54 Cal. App. 4th 121, 125, 62 Cal.Rptr.2d 620 (1997); see *Bureerong v. Uvawas*, 959 F.

Supp. 1231, 1237 (C.D. Cal. 1997) (“The Court disagrees with Hub’s broad and general contention that the Court may not recognize a negligence *per se* claim simply because the statute upon which the claim is based confers no private right of action.”) In other words, “it is the tort of negligence, and not the violation of the statute itself, which entitles a plaintiff to recover civil damages *1143 ... [T]he plaintiff is not attempting to pursue a private cause of action for violation of the statute; rather, he is pursuing a negligence action and is relying upon the violation of a statute, ordinance, or regulation to establish part of that cause of action.” *Sierra–Bay Fed. Land Bank Ass’n. v. Superior Court*, 227 Cal. App. 3d 318, 333, 277 Cal.Rptr. 753 (1991). Accordingly, Plaintiffs’ reliance on the negligence *per se* doctrine does not fail merely because the statutes they allege Defendants violated do not provide a private right of action. “Because Plaintiffs’ negligence cause of action may proceed, the Court does not dismiss the references to the negligence *per se* doctrine.” *Tinoco v. San Diego Gas & Elec. Co.*, 2018 WL 4562479, at *2 (S.D. Cal. Sept. 21, 2018).

D. Invasion of Privacy

[22] [23] To state a claim for invasion of privacy, “Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is ‘so serious ... as to constitute an egregious breach of the social norms’ such that the breach is ‘highly offensive.’” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020), *cert. denied sub nom. Facebook, Inc. v. Davis*, — U.S. —, 141 S. Ct. 1684, 209 L.Ed.2d 464 (2021). “Determining whether a defendant’s actions were ‘highly offensive to a reasonable person’ requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder’s motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.” *Id.* at 606.

[24] Plaintiffs have adequately alleged an invasion of privacy claim. In support of that claim, Plaintiffs allege that Defendants (1) knew their information security practices were inadequate and had numerous security vulnerabilities (SAC ¶¶ 300, 433, 486), (2) “intentionally, willfully, recklessly, or negligently” failed to take adequate and reasonable measures to ensure Ambry’s data systems were protected (*id.* ¶¶ 53–58), (3) knew their inadequate data security measures would likely result in a breach (*id.* ¶ 433), and (4) knew that such a breach would harm Plaintiffs (*id.* ¶ 434). Courts have refused to dismiss invasion of privacy claims at the motion to

dismiss stage where, as here, a data breach involved medical information, because the disclosure of such information is more likely to constitute an “egregious breach of the social norms” that is “highly offensive.” *See, e.g., Stasi*, 501 F. Supp. 3d at 926; *Doe v. Beard*, 63 F. Supp. 3d 1159, 1170 (C.D. Cal. 2014).

E. Breach of Express and Implied Contract

Plaintiffs allege that Defendants breached contracts including “test requisition forms, patient signature cards, HIPAA authorization forms, and patient consent forms,” in which Defendants “impliedly if not explicitly, agreed to protect Plaintiffs’ and other Class Members’ Private Information.” (SAC ¶¶ 439–40.) Plaintiffs alternatively allege that the parties “entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts concerning genetic testing or other services to be provided by Defendants to Plaintiffs.” (*Id.* ¶ 450.)

[25] [26] Defendants argue that Plaintiffs’ breach of express contract claim fails because “there is no independent contractual agreement in which KMPM or Ambry assumed obligations regarding data security or data breach notification.” (Mot. at 20.) The Court agrees. A claim for breach of contract “must allege the specific provisions in the contract creating the obligation *1144 the defendant is said to have breached.” *Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110, 1117 (N.D. Cal. 2011). Plaintiffs fail to do so. Rather, they state generally that “Ambry agreed to maintain Plaintiffs’ privacy in accordance with HIPAA and otherwise,” and did not. (Dkt. 104-1 [Opposition, hereinafter “Opp.”] at 25 [citing SAC ¶¶ 280–87].) The alleged contract terms do not contain promises from Defendants to keep Plaintiffs’ information safe. Instead, they are broad statements including “Ambry is committed to protecting the privacy of all users of the Services,” “Ambry Genetics cares about your patients and your data as much as you do,” “Information that you provide to Ambry through ambrygen.com is encrypted using industry standard Secure Sockets Layer (SSL) technology,” and “We are required by law to: Maintain the confidentiality of your protected health information in accordance with the Health Insurance Portability and Accountability Act of 1996 (‘HIPAA’) and applicable state law.” (SAC ¶¶ 280–84.) These allegations are not sufficient to allege a breach of express contract. *See Young*, 790 F. Supp. 2d at 1117.

[27] [28] [29] However, Plaintiffs have adequately stated a breach of implied contract. “An implied-in-fact contract requires proof of the same elements necessary to evidence

an express contract: mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter.” *Corona v. Sony Pictures Entm’t, Inc.*, 2015 WL 3916744, at *5 (C.D. Cal. June 15, 2015). “An implied contract requires that both parties agree to its terms and have a ‘meeting of the minds,’ but the creation of an implied contract can be manifested by conduct rather than words.” *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *8 (N.D. Cal. Sept. 14, 2016).

Plaintiffs allege that they gave their private information to Defendants for purposes of obtaining genetic testing, with the understanding that Defendants would take adequate measures to protect the information. “While [Defendants] made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient’s assent to protect the information sufficiently.” *Id.* at *9 (citing *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (holding that the plaintiffs had sufficiently pleaded “an implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to safeguard Plaintiffs’ personal and financial information”)); see *Rudolph v. Hudson’s Bay Co.*, 2019 WL 2023713, at *11 (S.D.N.Y. May 7, 2019) (“Other courts applying California law have concluded that an implied contract is formed where a person discloses sensitive information in order to receive a benefit, with the expectation that such information will be protected.”); *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *12 (S.D.N.Y. Aug. 4, 2021) (concluding that employees in data breach case failed to sufficiently state a claim for breach of express contract, but sufficiently stated a claim for breach of implied contract).

F. Unjust Enrichment

[30] “While California case law appears unsettled on the availability of [an independent unjust enrichment] cause of action, [the Ninth] Circuit has construed the common law to allow an unjust enrichment cause of action through quasi-contract.” *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016); see *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) (explaining *1145 that when a plaintiff alleges unjust enrichment, a court may “construe the cause of action as a quasi-contract claim seeking restitution”). “To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the

plaintiff’s expense.” *ESG Capital Partners, LP v. Stratos*, 828 F.3d 1023, 1038–39 (9th Cir. 2016); see *Bruton v. Gerber Prod. Co.*, 703 F. App’x 468, 470 (9th Cir. 2017) (reversing dismissal of an unjust enrichment claim in action regarding food labeling because “the California Supreme Court has clarified California law, allowing an independent claim for unjust enrichment to proceed in an insurance dispute”).

[31] “Courts have concluded that the failure to secure a plaintiff’s data can give rise to an unjust enrichment claim,” reasoning “that a defendant has accepted the benefits accompanying plaintiff’s data, but does so at the plaintiff’s expense by not implementing adequate safeguards, thus making it inequitable and unconscionable to permit defendant to retain funds that it saved by shirking data-security and leaving the plaintiff to suffer the consequences.” *Rudolph*, 2019 WL 2023713, at *12. This is exactly what Plaintiffs allege. Plaintiffs allege that they paid Defendants money for Defendants’ services, and expected that a portion of their payments would go toward “data management and security.” (SAC ¶¶ 461, 463.) They further allege that Defendants retained this benefit despite not having implemented adequate safeguards for Plaintiffs’ private information. (*Id.* ¶¶ 42, 464, 466.) This is sufficient to overcome a motion to dismiss. *Rudolph*, 2019 WL 2023713, at *12 (collecting cases); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016) (concluding that allegations that plaintiffs made payments to Premera expecting that a portion of their fees would be used for data management and security and that “under the circumstances it is unjust for Premera to retain the benefits received without payment” were “sufficient to withstand a motion to dismiss”).

G. Breach of Fiduciary Duty

[32] Plaintiffs allege that “Defendants have become a fiduciary, created by its undertaking and guardianship of patients’ Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members.” (SAC ¶ 473.) They further allege that Defendants breached their fiduciary duty to act for the benefit of Plaintiffs when they failed to protect Plaintiffs’ private information. (*Id.* ¶ 474.)

[33] [34] Defendants argue that Plaintiffs’ breach of fiduciary duty claim fails because they did not owe Plaintiffs a fiduciary duty. “A fiduciary relationship is any relation existing between parties to a transaction wherein one of the parties is duty bound to act with the utmost good faith for the benefit of the other party.” *Gilman v. Dalby*,

176 Cal. App. 4th 606, 613, 98 Cal.Rptr.3d 231 (2009). “[T]raditional examples of fiduciary relationships include those of trustee/beneficiary, corporate directors and majority shareholders, business partners, joint adventurers, and agent/principal.” *Id.* at 614, 98 Cal.Rptr.3d 231. “Inherent in each of these relationships is the duty of undivided loyalty the fiduciary owes to its beneficiary, imposing on the fiduciary obligations far more stringent than those required of ordinary contractors.” *Id.* (internal quotation omitted).

Plaintiffs have failed to allege sufficient facts to establish a fiduciary relationship between themselves and Defendants. Plaintiffs simply allege that Defendants collected Plaintiffs’ private information so Defendants could provide their genetic *1146 testing to screen for and [diagnose diseases](#). (See SAC ¶¶ 1, 473.) This is not a situation where the parties have a special relationship. See, e.g., [Giles v. Gen. Motors Acceptance Corp.](#), 494 F.3d 865, 883 (9th Cir. 2007) (finding no special relationship between plaintiff car dealership operators and representative from defendant wholesale car financier, even though plaintiffs alleged that they placed a “special trust” or “special confidence” in the representative, because the relationship was “a standard friendly but arms-length business relationship”). Nor is the relationship alleged between the parties one in which Defendants assumed obligations to act with the utmost good faith for the benefit of Plaintiffs. Defendants never “agreed to subordinate [their] interests to those of Plaintiff[s],” and Plaintiffs were not “so vulnerable as to give rise to equitable concerns underlying the protection afforded by law governing fiduciaries.” [ReactX v. Mendez](#), 2018 WL 6164275, at *6 (C.D. Cal. Jan. 4, 2018). Rather, Plaintiffs entered into an arms-length business relationship with Defendants, which is insufficient to create a fiduciary duty even though Plaintiffs entrusted Defendants with their confidential information as part of the relationship. [Giles](#), 494 F.3d at 883; see [Worldvision Enterprises, Inc. v. Am. Broad. Companies, Inc.](#), 142 Cal. App. 3d 589, 595, 191 Cal.Rptr. 148 (1983) (“The mere fact that in the course of their business relationships the parties reposed trust and confidence in each other does not impose any corresponding fiduciary duty in the absence of an act creating or establishing a fiduciary relationship known to law.”); [Anderson v. Hannaford Bros. Co.](#), 659 F.3d 151, 157 (1st Cir. 2011) (rejecting contention that “a fiduciary relationship arises in the context of credit and debit card use because the customer trusts the merchant to safeguard her credit or debit card information”).

H. Breach of Confidence

[35] [36] The tort for breach of confidence under California law “is based upon the concept of an implied obligation or contract between the parties that confidential information will not be disclosed.” [Ent. Rsch. Grp., Inc. v. Genesis Creative Grp., Inc.](#), 122 F.3d 1211, 1226–27 (9th Cir. 1997). To sufficiently allege a breach of confidence claim, a plaintiff must allege that “(1) the plaintiff conveyed ‘confidential and novel information’ to the defendant; (2) the defendant had knowledge that the information was being disclosed in confidence; (3) there was an understanding between the defendant and the plaintiff that the confidence be maintained; and (4) there was a disclosure or use in violation of the understanding.” *Id.* at 1227.

[37] Defendants argue that Plaintiffs’ breach of confidence claim fails because Plaintiffs do not allege that Defendants gave their private information away, but rather allege that the information was involuntarily stolen from Defendants. (Mot. at 25–26.) The Court agrees. The question turns on the meaning of the word “disclosure” in the fourth element. California courts have found that the “ordinary meaning” of the word “disclosure” “suggest[s] that disclosure occurs when the health care provider affirmatively shares medical information with another person or entity.” [Sutter Health v. Superior Ct.](#), 227 Cal. App. 4th 1546, 1555–56, 174 Cal.Rptr.3d 653 (2014); see [In re Brinker Data Incident Litig.](#), 2020 WL 691848, at *22 (M.D. Fla. Jan. 27, 2020) (“According to Black’s Law Dictionary, ‘disclosure’ is ‘[t]he act or process of making known something that was previously unknown.’”).

Here, Plaintiffs allege that “unauthorized parties accessed the email account of *1147 an Ambry employee allowing unauthorized parties to access and acquire Plaintiffs’ and Class Members’ Private Information.” (SAC ¶ 66.) Plaintiffs do not allege that Defendants affirmatively shared any information or performed any act that gave hackers information. Since Defendants made no “disclosure” of Plaintiffs’ confidential information, they cannot be held liable on a claim for breach of confidence. See [In re Brinker Data Incident Litig.](#), 2020 WL 691848, at *22 (dismissing breach of confidence claim where the plaintiff “did not do any act that made Plaintiffs’ information known—the information was stolen by third-parties”).

I. Unfair Competition Law

[38] [39] [40] Plaintiff’s eighth claim alleges a violation of California’s UCL, which prohibits “any unlawful, unfair or fraudulent business act or practice and unfair, deceptive,

untrue or misleading advertising.” *Cal. Bus. & Prof. Code § 17200*. Remedies under the UCL are limited to restitution and injunctive relief, and do not include damages. *Silvercrest Realty, Inc. v. Great Am. E&S Ins. Co.*, 2012 WL 13028094, at *2 (C.D. Cal. Apr. 4, 2012). Restitution and injunctive relief are equitable remedies, and thus are not available unless the plaintiff lacks an adequate remedy at law. *Id.* A plaintiff “must establish that she lacks an adequate remedy at law before securing equitable restitution for past harm under the UCL.” *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020).

[41] Plaintiff alleges that “[b]y reason of Defendants’ ... wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class members’ Private Information, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.” (SAC ¶ 491.) Defendants argue that Plaintiffs’ UCL claim must be dismissed because Plaintiffs fail to allege they lack an adequate legal remedy for the harm sustained from the data breach. (Mot. at 27.) The Court agrees.

Plaintiffs’ UCL claim is based on the allegation that Defendants failed to take adequate measures to protect Plaintiffs’ private information—Defendants’ *past* conduct—not any allegation that Defendants are failing to prevent *future* data breaches. Specifically, Plaintiffs allege that Defendants’ business practices are unfair because they are “immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the Private Information of Plaintiffs and Class Members has been compromised for unauthorized parties to see, use, and otherwise exploit.” (SAC ¶ 493.) They allege Defendants’ business practices are unlawful “because Defendants failed to take reasonable measures to protect Plaintiffs’ and Class Members’ Private Information and failed to take remedial measures such as notifying its users when it first discovered that their Private Information may have been compromised.” (*Id.* ¶ 496.) And they allege Defendants’ business practices are fraudulent because they deceived consumers into believing their private information would remain secure. (*Id.* ¶ 498.) Throughout their SAC, Plaintiffs seek compensatory damages for this past harm. Plaintiffs have failed to allege that the legal remedies they seek for the injuries they incurred as a result of Defendants’ past failure to protect their information are inadequate.

J. Confidentiality of Medical Information Act

Plaintiffs allege violations of two provisions of the CMIA: *Section 56.10*, which prohibits disclosure of medical information without prior authorization, and *1148 *Section 56.101*, which penalizes negligently maintaining or storing medical information.

1. Section 56.10

[42] [43] Plaintiffs first allege that “Defendants’ misuse and/or disclosure of medical information regarding Plaintiffs and Class Members constitutes a violation of *Civil Code § 56.10*.” (SAC ¶ 514.) *Section 56.10* states, “A provider of health care, health care service plan, or contractor shall not **disclose** medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization.” *Cal. Civ. Code § 56.10* (emphasis added). “Disclosure” in this context “refers to affirmative communicative acts—giving out medical information on a patient.” *Sutter Health*, 227 Cal. App. 4th at 1554, 174 Cal.Rptr.3d 653; see *Regents of Univ. of California v. Superior Ct.*, 220 Cal. App. 4th 549, 564, 163 Cal.Rptr.3d 205 (2013), as modified on denial of reh’g (Nov. 13, 2013) (“Disclose” ... is an active verb, denoting in the context of CMIA and the protections afforded confidential medical information an affirmative act of communication.”).

Here, as already explained, Plaintiffs allege that hackers gained unauthorized access to an Ambry employee’s email account. They do not allege that Defendants performed any affirmative communicative act that gave hackers information. See *Sutter Health*, 227 Cal. App. 4th at 1554, 174 Cal.Rptr.3d 653; *Regents*, 220 Cal. App. 4th at 564, 163 Cal.Rptr.3d 205. Accordingly, Plaintiff’s claim under *Section 56.10* fails. See *Stasi*, 501 F. Supp. 3d at 922 (“Based on the meaning of ‘disclose’ as defined in *Sutter* and *Regents*, Plaintiffs have not pled a plausible violation of *section 56.10(a)* of CMIA.”).

2. Section 56.101

[44] [45] However, Plaintiffs allege that Defendants also violated *Section 56.101* of the CMIA. (SAC ¶ 517.) *Section 56.101* penalizes those who **negligently** maintain or store medical information. *Cal. Civ. Code § 56.101* (emphasis added). Under *Section 56.36*, an individual may bring an action for damages against an entity that has negligently released confidential information or records. In contrast to disclosure under *Section 56.10*, “negligent release under

section 56.36 does not require an affirmative communicative act but instead can be accomplished by negligently allowing information to end up in the possession of an unauthorized person.” *Sutter Health*, 227 Cal. App. 4th at 1554–55, 174 Cal.Rptr.3d 653. A plaintiff must allege that a defendant’s “negligence result[ed] in unauthorized or wrongful access to the information,” i.e. that the information was “improperly viewed or otherwise accessed.” *Regents*, 220 Cal. App. 4th at 554, 163 Cal.Rptr.3d 205; see *Sutter Health*, 227 Cal. App. 4th at 1557, 174 Cal.Rptr.3d 653 (“No breach of confidentiality takes place until an unauthorized person views the medical information.”).

[46] Defendants argue that Plaintiffs’ claim under Section 56.101 must be dismissed because Plaintiffs do not sufficiently allege that their information was viewed by third parties. (Mot. at 32–33.) But Plaintiffs do so allege: they allege that “unauthorized parties have accessed and viewed Plaintiffs’ and Class Members’ unencrypted, unredacted information, including ... relevant medical records.” (SAC ¶ 76; see *id.* ¶ 92 [“Plaintiffs’ and Class Members’ unencrypted personal information that was acquired by an unauthorized person as a result of the Data Breach, was viewed by unauthorized persons.”]; *id.* ¶ 512 [“The hacker or hackers who committed the Data Breach obtained Plaintiffs’ and Class Members’ personal medical information, viewed it, and now have it available to them to sell to others bad actors or *1149 otherwise misuse.”].) At the pleading stage, Plaintiffs have sufficiently stated a claim under Section 56.101. See *Stasi*, 501 F. Supp. 3d at 924 (“Ultimately, it may be that Plaintiffs’ allegation that their information was actually viewed while it was accessible on the internet will prove to be unsubstantiated. At this early stage in the litigation, however, Plaintiffs allege a plausible claim based on violations of sections 56.101(a) and 56.36(b) of CMIA.”).

K. Consumer Legal Remedies Act

The CLRA makes unlawful “unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer.” Cal. Civ. Code § 1770. For example, as relevant here, it is unlawful to “represent[] that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have.” Cal. Civ. Code § 1770(a)(5).

[47] Plaintiffs’ CLRA claim fails for the same reasons their UCL claim fails. Specifically, the claim is targeted at Defendants’ past conduct. Plaintiffs allege that Defendants violated the CLRA by representing that they took appropriate measures to protect Plaintiffs’ private information, but then failing to protect the information. (SAC ¶ 527.) Plaintiffs fail to allege that the legal remedies they seek to redress that past conduct are inadequate. See *Sonner*, 971 F.3d at 844 (“A plaintiff “must establish that she lacks an adequate remedy at law before securing equitable restitution for past harm under the UCL and CLRA.”); Section III.I., *supra*.

Defendants also argue that Plaintiffs’ CLRA claim fails because Plaintiffs failed to comply with the CLRA’s pre-filing requirements. (Mot. at 35–36.) The CLRA requires that at least 30 days before filing a CLRA action, a plaintiff must notify the person alleged to have violated Section 1770 of the particular violations alleged, and also demand that the person correct, repair, replace, or otherwise rectify the goods or services alleged to be in violation of Section 1770. Cal. Civ. Code § 1782. Plaintiffs do not dispute that they did not comply with the CLRA’s notice requirements. (See Opp. at 35–36.) Rather, Plaintiffs allege that “Defendants have long had notice of Plaintiffs’ allegations, claims and demands, including from the filing of numerous underlying actions against it arising from the Data Breach, the first of which were filed on or about April 22, 2020,” and that “Defendants are the parties with the most knowledge of the underlying facts giving rise to Plaintiffs’ allegations, so that any pre-suit notice would not put Defendants in a better position to evaluate those claims.” (SAC ¶ 522.) But Plaintiffs cite no authority showing that the CLRA’s notice requirements may be excused in such a situation, and the SAC admits that Plaintiffs have not complied with the statutory requirements.

L. Consumer Records Act

[48] The CRA requires California businesses that own or license computerized data that includes personal information to disclose a data breach after discovering one “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, ... or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” Cal. Civ. Code § 1798.82. Plaintiffs allege that “Defendants unreasonably delayed informing Plaintiffs and Class *1150 Members about the Data Breach.” (SAC ¶ 540.)

Defendants argue that Plaintiffs fail to sufficiently allege unreasonable delay because Defendants’ delay is explained

by their need to “take measures to first determine the breach’s scope and restore the integrity of the data system.” (Mot. at 38); see [Cal. Civ. Code § 1798.82](#). However, at the pleading stage the Court must accept as true Plaintiffs’ allegation that Defendants’ approximately 3-month delay was unreasonable. More specifically, Plaintiffs allege that Defendants’ delay prevented them from taking appropriate protective measures that could have prevented some of the damages they suffered, and that they therefore suffered “incrementally increased damages” that they would not have suffered with timelier notice. (SAC ¶¶ 544–45.) Indeed, some Plaintiffs allege that they suffered injuries resulting from the breach before they were notified of it that they might have been able to take steps to avoid had they been notified sooner. (See, e.g., *id.* ¶¶ 142 [Coleman], 263 [Terrano].) Plaintiffs therefore sufficiently allege that Defendants’ delay caused them to incur more damages than they would have incurred with timely notice.

[49] Finally, Defendants argue that Plaintiffs’ CRA claim should be dismissed insofar as Plaintiffs seek to assert it on behalf of non-California residents. Defendants are right on this point. “[D]istrict courts have dismissed CRA claims brought on behalf of non-California Plaintiffs because the CRA is clear that it applies only to ensure the personal information of California residents is protected.” *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *34 (N.D. Cal. Aug. 30, 2017) (cleaned up) (collecting cases). Plaintiffs do not argue otherwise. (See Opp. at 37.) Accordingly, Plaintiffs’ CRA claim may only be asserted on behalf of California residents.

M. Illinois Genetic Information Privacy Act

The IGIPA provides that “genetic testing and information derived from genetic testing is confidential and privileged and may be released only to the individual tested and to persons specifically authorized, in writing in accordance with Section 30, by that individual to receive the information.” [410 Ill. Comp. Stat. Ann. 513/15](#). It further requires that “[w]hen using or disclosing genetic-related information under this Act, a covered entity shall do so in accordance with the minimum necessary standard under HIPAA.” [410 Ill. Comp. Stat. Ann. 513/31.10](#). Finally, it states that “[n]o person may disclose ... the identity of any person upon whom a genetic test is performed or the results of a genetic test in a manner that permits identification of the subject of the test.” [410 Ill. Comp. Stat. Ann. 513/30](#). Plaintiffs allege, on behalf of Plaintiff Taglioli and the Illinois sub-class, that Defendants violated each of these provisions “[b]y disclosing Plaintiffs’

and Class Members’ Private Information to unauthorized parties.” (SAC ¶ 553.)

[50] [51] For the same reasons described in Sections III.H. and III.J.1., Plaintiffs have not sufficiently alleged *disclosure* of their private information. Thus, Plaintiffs may not pursue a claim under [410 Ill. Comp. Stat. Ann. 513/31.10](#) or [410 Ill. Comp. Stat. Ann. 513/30](#). But Plaintiffs can state a claim under [410 Ill. Comp. Stat. Ann. 513/15](#), which governs to whom genetic testing and information derived from genetic testing may be *released*. Defendants argue that Plaintiffs have failed to allege any harm stemming from the disclosure of their genetic information, as Plaintiffs allege harm in the form of identity theft and fraud, not harm occurring *1151 from the disclosure of genetic information. Plaintiffs, however, have alleged harm stemming from disclosure of their genetic information—harm to their privacy interests in that information. (See, e.g., SAC ¶¶ 119, 124, 129); see *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019), *cert. denied*, — U.S. —, 140 S. Ct. 937, 205 L.Ed.2d 524 (2020) (finding that plaintiffs had standing “[b]ecause the privacy right protected by BIPA¹ is the right not to be subject to the collection and use of such biometric data,” and therefore “Facebook’s alleged violation of these statutory requirements would necessarily violate the plaintiffs’ substantive privacy interests”).

[52] Defendants also argue that Plaintiffs fail to allege that the information the IGIPA protects—information derived from genetic testing—was released. (Mot. at 42.) But Plaintiffs allege that “medical information” and “diagnosis information” were released in the breach. (SAC ¶ 71.) Given that Defendants are a genetic testing company, it is plausible that information derived from genetic testing was among the medical information and diagnosis information released in the breach.

N. Injunctive and Declaratory Relief

Plaintiffs’ final claim in their SAC is for “Injunctive and Declaratory Relief.” Defendants argue that this claim must be dismissed because Plaintiffs have failed to show that they lack an adequate remedy at law. (Mot. at 43–44.) But as already explained, Plaintiffs may seek both damages for past harm and injunctive relief to prevent future harm. See Section III.B.2., *supra*; see also Sections III.I. and III.K., *supra* (explaining that to the extent Plaintiffs failed to allege they lacked an adequate remedy at law in support of their UCL and CLRA claims, it was because those claims sought relief

based on Defendants' past conduct, not relief to prevent future harm).

O. Leave to Amend

[53] "Although leave to amend 'shall be freely given when justice so requires,' it may be denied" where it "would not serve any purpose because to grant it would be futile in saving the plaintiff's suit." *Chinatown Neighborhood Ass'n v. Harris*, 794 F.3d 1136, 1144 (9th Cir. 2015) (quoting Fed. R. Civ. P. 15(a)). For some of Plaintiffs' claims, leave to amend is not appropriate. This is Defendants' *fourth* motion to dismiss Plaintiffs' complaints—Defendants moved to dismiss Plaintiffs' Consolidated Complaint (Dkt. 43), their First Amended Consolidated Complaint (Dkt. 63), their Second Amended Consolidated Complaint (Dkt. 75), and their Second Amended Consolidated Complaint a second time by this motion. With limited exception, each of those motions raised the arguments presented in this motion. Plaintiffs have failed to cure the deficiencies in the dismissed claims despite multiple opportunities to do so, and nothing in the record suggests that they could allege any new facts that would suffice to plausibly state most of these claims.

[54] Recognizing this, Plaintiffs seek leave to amend only their UCL claim, asserting that Defendants' argument based on *Sonner* was raised for the first time in this motion to dismiss. (Opp. at 31.) The Court will grant this request. Since

the Court granted Defendants' motion on Plaintiffs' CLRA claim on the same basis *1152 as Plaintiffs' UCL claim, the Court will also permit amendment of that claim.

IV. CONCLUSION

For the foregoing reasons, Defendants' motion to dismiss is **GRANTED IN PART AND DENIED IN PART**. Defendants' motion is **GRANTED** as to Plaintiffs' claim against KMPM on the theory that it failed to engage in due diligence before it existed, and Plaintiffs' claims for breach of express contract, breach of fiduciary duty, breach of confidence, violation of the UCL, violation of Section 56.10 of the CMIA, violation of the CLRA, and violation of the CRA as to non-California residents. Defendants' motion is **DENIED** as to Plaintiffs' claim against KMPM on the theory that it failed to take action after it had come into existence based on due diligence, and Plaintiffs' claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, violation of Section 56.101 of the CMIA, violation of the CRA as to California residents, violation of the IGIPA, and injunctive and declaratory relief. Plaintiffs' request for leave to amend is **GRANTED** as to Plaintiffs' claims under the UCL and CLRA only.

All Citations

567 F.Supp.3d 1130

Footnotes

- 1 The parties agree that courts consider the IGIPA as similar to the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/10, 14/1 ("BIPA"), as both statutes were created at the same time and feature the same language for a private right of action for an "aggrieved" party. (Mot. at 40; Opp. at 39.)

43 F.4th 1207

United States Court of Appeals, Federal Circuit.

Stephen THALER, Plaintiff-Appellant

v.

Katherine K. VIDAL, Under Secretary of
Commerce for Intellectual Property and
Director of the [United States Patent and
Trademark Office, United States Patent and
Trademark Office](#), Defendants-Appellees

2021-2347

|

Decided: August 5, 2022

Synopsis

Background: Applicant, who filed two patent applications listing artificial intelligence (AI) software system as sole inventor, sought judicial review of decisions of the United States Patent and Trademark Office (PTO) to deny applications on the ground that AI software system did not qualify as inventor. The United States District Court for the Eastern District of Virginia, [Leonie M. Brinkema, J.](#), [558 F.Supp.3d 238](#), granted PTO's motion for summary judgment and denied applicant's request to reinstate his applications. Applicant appealed.

[Holding:] The Court of Appeals, [Stark](#), Circuit Judge, held that Patent Act requires that inventors listed on patent applications be natural persons.

Affirmed.

Procedural Posture(s): On Appeal; Motion for Summary Judgment; Review of Administrative Decision.

West Headnotes (10)

[1] Courts [Particular questions or subject matter](#)

Court of Appeals for the Federal Circuit reviews grants of summary judgment according to the law of the regional circuit.

[2] Federal Courts [Summary judgment](#)

In the Fourth Circuit, a district court's grant of summary judgment is reviewed de novo.

[3] Patents [Scope of Review](#)

Challenges to United States Patent and Trademark Office (PTO) petition decisions are governed by the Administrative Procedure Act (APA) and pertinent administrative law standards. [5 U.S.C.A. § 706](#).

[4] Federal Courts [Statutes, regulations, and ordinances, questions concerning in general](#)

Statutory interpretation is an issue of law that Court of Appeals reviews de novo.

[5] Statutes [Language](#)

Statutes [Absence of Ambiguity; Application of Clear or Unambiguous Statute or Language](#)

In resolving disputes of statutory interpretation, courts begin with the statutory text, and end there as well if the text is unambiguous.

[2 Cases that cite this headnote](#)

[6] Patents [Persons Entitled to Patents](#)

The Patent Act requires that inventors listed on patent applications be natural persons; that is, human beings. [35 U.S.C.A. §§ 100\(f\), 100\(g\), 115](#).

[4 Cases that cite this headnote](#)

[7] Statutes [Persons or Entities Subject](#)

When used as a noun in a statute, "individual" ordinarily means a human being, a person.

[1 Case that cites this headnote](#)

[8] Patents 🔑 Purpose and construction in general

In the Patent Act, “individuals” and, thus, “inventors” are natural persons. 35 U.S.C.A. §§ 100(f), 100(g), 115.

[4 Cases that cite this headnote](#)

[9] Statutes 🔑 Language and intent, will, purpose, or policy

When interpreting a statute, courts may not elevate vague invocations of statutory purpose over the words Congress chose.

[10] Constitutional Law 🔑 Limitations of Rules and Special Circumstances Affecting Them**Patents** 🔑 Purpose and construction in general

Canon of constitutional avoidance did not apply to overcome interpretation of unambiguous term “inventor” in the Patent Act as being limited to natural persons; federal constitution granted legislative power to Congress to promote the progress of science and useful arts by securing to inventors the exclusive right to writings and discoveries, and Congress chose to act pursuant to that power by passing the Patent Act. U.S. Const. art. 1, § 8, cl. 8; 35 U.S.C.A. §§ 100(f), 100(g).

[3 Cases that cite this headnote](#)

[More cases on this issue](#)

***1208** Appeal from the United States District Court for the Eastern District of Virginia in No. 1:20-cv-00903-LMB-TCB, Judge [Leonie M. Brinkema](#).

Attorneys and Law Firms

[Ryan Benjamin Abbott](#), Brown, Neri, Smith & Khan, LLP, Los Angeles, CA, argued for plaintiff-appellant.

[Dennis Barghaan, Jr.](#), Office of the United States Attorney for the Eastern District of Virginia, United States Department of Justice, Alexandria, VA, argued for defendants-appellees.

Also represented by Jessica D. Aber; [Farheena Yasmeen Rasheed](#), [Peter John Sawert](#), Meredith Hope Schoenfeld, Office of the Solicitor, United States Patent and Trademark Office, Alexandria, VA.

Mitchell Apper, Jerusalem, Israel, amicus curiae, pro se.

Before [Moore](#), Chief Judge, [Taranto](#) and [Stark](#), Circuit Judges.

Opinion

[Stark](#), Circuit Judge.

***1209** This case presents the question of who, or what, can be an inventor. Specifically, we are asked to decide if an artificial intelligence (AI) software system can be listed as the inventor on a patent application. At first, it might seem that resolving this issue would involve an abstract inquiry into the nature of invention or the rights, if any, of AI systems. In fact, however, we do not need to ponder these metaphysical matters. Instead, our task begins – and ends – with consideration of the applicable definition in the relevant statute.

The United States Patent and Trademark Office (PTO) undertook the same analysis and concluded that the Patent Act defines “inventor” as limited to natural persons; that is, human beings. Accordingly, the PTO denied Stephen Thaler's patent applications, which failed to list any human as an inventor. Thaler challenged that conclusion in the U.S. District Court for the Eastern District of Virginia, which agreed with the PTO and granted it summary judgment. We, too, conclude that the Patent Act requires an “inventor” to be a natural person and, therefore, affirm.

I

Thaler represents that he develops and runs AI systems that generate patentable inventions. One such system is his “Device for the Autonomous Bootstrapping of Unified Science,” which Thaler calls “DABUS.” Thaler has described DABUS as “a collection of source code or programming and a software program.” Supp. App. at 781.

In July 2019, Thaler sought patent protection for two of DABUS' putative inventions by filing two patent applications with the PTO: U.S. Application Nos. 16/524,350 (teaching a “Neural Flame”) and 16/524,532 (teaching a “Fractal

Container”).¹ He listed DABUS as the sole inventor on both applications. Thaler maintains that he did not contribute to the conception of these inventions and that any person having skill in the art could have taken DABUS' output and reduced the ideas in the applications to practice.²

In lieu of an inventor's last name, Thaler wrote on the applications that “the invention [was] generated by artificial intelligence.” App. at 28, 69. He also attached several documents relevant to inventorship. First, to satisfy 35 U.S.C. § 115's requirement that inventors submit a sworn oath or declaration when applying for a patent, Thaler submitted a statement on DABUS' behalf. Second, Thaler provided a supplemental “Statement on Inventorship” explaining that DABUS was “a particular type of connectionist artificial intelligence” *1210 called a “Creativity Machine.” App. at 198-203, 483-88. Third, Thaler filed a document purporting to assign himself all of DABUS' rights as an inventor.

The PTO concluded both applications lacked a valid inventor and were, hence, incomplete. Accordingly, it sent Thaler a “Notice to File Missing Parts of Nonprovisional Application” for each application and requested that Thaler identify valid inventors. In response, Thaler petitioned the PTO director to vacate the Notices based on his Statements of Inventorship. The PTO denied Thaler's petitions on the ground that “a machine does not qualify as an inventor.” App. at 269-71, 548-50. Thaler sought reconsideration, which the PTO denied, explaining again that inventors on a patent application must be natural persons.

Thaler then pursued judicial review of the PTO's final decisions on his petitions, under the Administrative Procedure Act (APA). See 5 U.S.C. §§ 702-704, 706.³ The parties agreed to have the District Court adjudicate the challenge based on the administrative record made before the PTO and filed cross-motions for summary judgment. After briefing and oral argument, the Court granted the PTO's motion for summary judgment and denied Thaler's request to reinstate his applications. The District Court concluded that an “inventor” under the Patent Act must be an “individual” and the plain meaning of “individual” as used in the statute is a natural person.

Thaler appealed. We have jurisdiction under 28 U.S.C. § 1295. See *Odysey Logistics & Tech. Corp. v. Iancu*, 959 F.3d 1104, 1108 (Fed. Cir. 2020) (explaining that Federal Circuit has jurisdiction over appeals from district court decisions raising APA claims against PTO regarding patents).

II

[1] [2] [3] [4] We review grants of summary judgment according to the law of the regional circuit, in this case the Fourth Circuit. See *Supernus Pharms., Inc. v. Iancu*, 913 F.3d 1351, 1356 (Fed. Cir. 2019). In the Fourth Circuit, a district court's grant of summary judgment is reviewed *de novo*. See *id.* (citing *Gallagher v. Reliance Standard Life Ins. Co.*, 305 F.3d 264, 268 (4th Cir. 2002)). Challenges to PTO petition decisions are governed by the APA and pertinent administrative law standards. Thus, we may set aside the judgment resulting from an administrative adjudication only if the agency's decision is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law” or if the agency's actions are “in excess of statutory jurisdiction, authority, or limitations.” 5 U.S.C. § 706. “Statutory interpretation is an issue of law that we review *de novo*.” *Facebook, Inc. v. Windy City Innovations, LLC*, 973 F.3d 1321, 1330 (Fed. Cir. 2020).

A

[5] [6] The sole issue on appeal is whether an AI software system can be an “inventor” under the Patent Act. In resolving disputes of statutory interpretation, we “begin[] with the statutory text, and end[] there as well if the text is unambiguous.” *BedRoc Ltd. v. United States*, 541 U.S. 176, 183, 124 S.Ct. 1587, 158 L.Ed.2d 338 (2004). Here, there is no ambiguity: the Patent Act requires that inventors must be natural persons; that is, human beings.

*1211 The Patent Act expressly provides that inventors are “individuals.” Since 2011, with the passage of the Leahy-Smith America Invents Act, the Patent Act has defined an “inventor” as “the *individual* or, if a joint invention, the *individuals* collectively who invented or discovered the subject matter of the invention.” 35 U.S.C. § 100(f) (emphasis added). The Act similarly defines “joint inventor” and “coinventor” as “any 1 of the *individuals* who invented or discovered the subject matter of a joint invention.” § 100(g) (emphasis added). In describing the statements required of an inventor when applying for a patent, the statute consistently refers to inventors and co-inventors as “individuals.” See § 115.

[7] The Patent Act does not define “individual.” However, as the Supreme Court has explained, when used “[a]s a noun, ‘individual’ ordinarily means a human being, a person.” *Mohamad v. Palestinian Auth.*, 566 U.S. 449, 454, 132 S.Ct. 1702, 182 L.Ed.2d 720 (2012) (internal alteration and quotation marks omitted). This is in accord with “how we use the word in everyday parlance”: “We say ‘the individual went to the store,’ ‘the individual left the room,’ and ‘the individual took the car,’ each time referring unmistakably to a natural person.” *Id.* Dictionaries confirm that this is the common understanding of the word. *See, e.g., Individual, Oxford English Dictionary* (2022) (giving first definition of “individual” as “[a] single human being”); *Individual, Dictionary.com* (last visited July 11, 2022), <https://www.dictionary.com/browse/individual> (giving “a single human being, as distinguished from a group” as first definition for “individual”). So, too, does the Dictionary Act, which provides that legislative use of the words “person” and “whoever” broadly include (“unless the context indicates otherwise”) “corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals.” 1 U.S.C. § 1 (emphasis added). “With the phrase ‘as well as,’ the definition marks ‘individual’ as distinct from the list of artificial entities that precedes it,” showing that Congress understands “individual” to indicate natural persons unless otherwise noted. *Mohamad*, 566 U.S. at 454, 132 S.Ct. 1702.

Consequently, the Supreme Court has held that, when used in statutes, the word “individual” refers to human beings unless there is “some indication Congress intended” a different reading. *Id.* at 455, 132 S.Ct. 1702 (emphasis omitted).⁴ Nothing in the Patent Act indicates Congress intended to deviate from the default meaning. To the contrary, the rest of the Patent Act supports the conclusion that “individual” in the Act refers to human beings.

For instance, the Act uses personal pronouns – “himself” and “herself” – to refer to an “individual.” § 115(b)(2). It does not also use “itself,” which it would have done if Congress intended to permit non-human inventors. The Patent Act also requires inventors (unless deceased, incapacitated, or unavailable) to submit an oath or declaration. *See, e.g., id.* (requiring oath or declaration from inventor that “such individual believes himself or herself to be the original inventor or an original joint inventor of a claimed invention in the application”). While we do not decide whether an AI system can form beliefs, nothing in our record shows that one

can, as reflected in the fact that Thaler submitted the requisite statements himself, purportedly on DABUS’ behalf.

*1212 Thaler directs us to several provisions of the Patent Act as supposed support for his position that “inventor” should be broadly read to include AI software, but each fails to persuade. First, Thaler points to the use of “whoever” in 35 U.S.C. §§ 101 and 271. Section 101 provides that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” As this very section makes clear, however, patents must satisfy the “conditions and requirements of” Title 35 of the U.S. Code, including its definition of “inventor.” Section 271, in setting out what constitutes infringement, repeatedly uses “whoever” to include corporations and other non-human entities. That non-humans may infringe patents does not tell us anything about whether non-humans may also be inventors of patents. The question before us inevitably leads back to the Patent Act’s definition of “inventor,” which uses the word “individual” – and does not use “whoever.”⁵ Furthermore, as we noted already, the Dictionary Act establishes that Congress uses “whoever” as a much broader term than “individual.” *See* 1 U.S.C. § 1.

Second, Thaler contends that AI software programs must qualify as inventors because otherwise patentability would depend on “the manner in which the invention was made,” in contravention of 35 U.S.C. § 103. Section 103 is not about inventorship. Instead, it provides, in relevant part, that inventions may still be nonobvious even if they are discovered during “routine” testing or experimentation. *See Honeywell Int’l Inc. v. Mexichem Amanco Holding S.A. de C.V.*, 865 F.3d 1348, 1356 (Fed. Cir. 2017); *see also Graham v. John Deere Co.*, 383 U.S. 1, 15, 86 S.Ct. 684, 15 L.Ed.2d 545 (1966) (explaining that second sentence of § 103 was intended to clarify that “flash of creative genius” is unnecessary for patentability). This statutory provision relates to *how* an invention is made and does not trump a provision that specifically addresses *who* may be an inventor.

Third, Thaler emphasizes that the term “inventor” must be interpreted with attention to the “context in which that language is used[] and the broader context of the statute as a whole.” *Yates v. United States*, 574 U.S. 528, 537, 135 S.Ct. 1074, 191 L.Ed.2d 64 (2015) (internal quotation marks omitted). We have undertaken precisely this task. For the

reasons explained above, the Patent Act, when considered in its entirety, confirms that “inventors” must be human beings.

B

Our holding today that an “inventor” must be a human being is supported by our own precedent. See *Univ. of Utah v. Max-Planck-Gesellschaft zur Forderung der Wissenschaften E.V.*, 734 F.3d 1315, 1323 (Fed. Cir. 2013) (“[I]nventors must be *natural persons* and cannot be corporations or sovereigns.”) (emphasis added); *Beech Aircraft Corp. v. EDO Corp.*, 990 F.2d 1237, 1248 (Fed. Cir. 1993) (“[O]nly natural persons can be ‘inventors.’”). While these opinions addressed different questions – concluding that neither corporations nor sovereigns can be inventors – our reasoning did not depend on the fact that institutions are collective entities. The two cases confirm that the plain meaning of “inventor” in the Patent Act is limited to natural persons.

*1213 C

[8] Statutes are often open to multiple reasonable readings. Not so here. This is a case in which the question of statutory interpretation begins and ends with the plain meaning of the text. See *Bostock v. Clayton Cnty.*, — U.S. —, 140 S. Ct. 1731, 1749, 207 L.Ed.2d 218 (2020) (“This Court has explained many times over many years, when the meaning of the statute’s terms is plain, our job is at an end.”). In the Patent Act, “individuals” – and, thus, “inventors” – are unambiguously natural persons. Accordingly, we have no need to consider additional tools of statutory construction. See *Matal v. Tam*, — U.S. —, 137 S. Ct. 1744, 1756, 198 L.Ed.2d 366 (2017) (“[I]nquiry into the meaning of the statute’s text ceases when the statutory language is unambiguous and the statutory scheme is coherent and consistent.”) (internal quotation marks omitted).

III

We briefly address Thaler’s additional arguments.

[9] Thaler argues that inventions generated by AI should be patentable in order to encourage innovation and public disclosure. Thaler’s policy arguments are speculative and lack a basis in the text of the Patent Act and in the record. In any event, the text before us is unambiguous, and we

may not “elevate vague invocations of statutory purpose over the words Congress chose.” *Sw. Airlines Co. v. Saxon*, — U.S. —, 142 S. Ct. 1783, 1792-93, 213 L.Ed.2d 27 (2022). Moreover, we are not confronted today with the question of whether inventions made by human beings with the *assistance* of AI are eligible for patent protection.

[10] Thaler invokes the canon of constitutional avoidance. In Thaler’s view, permitting AI programs to be inventors would support the constitutional purpose of patents “[t]o promote the progress of science and the useful arts.” U.S. Const. art. I, § 8, cl. 8. It follows, Thaler continues, that not recognizing AI as an inventor undermines such progress, raising potential constitutional concerns we should be careful to avoid. Thaler is incorrect. The constitutional provision he cites is a grant of legislative power to Congress; Congress has chosen to act pursuant to that power by passing the Patent Act. Thaler does not (and cannot) argue that limiting inventorship to human beings is unconstitutional. Therefore, the canon of constitutional avoidance is simply inapplicable. See *Veterans4You LLC v. United States*, 985 F.3d 850, 860-61 (Fed. Cir. 2021) (explaining that this canon may be helpful when there is serious question regarding statute’s constitutionality); see also *Warger v. Shauers*, 574 U.S. 40, 50, 135 S.Ct. 521, 190 L.Ed.2d 422 (2014) (noting that canon of constitutional avoidance “has no application in the absence of ... ambiguity”) (internal quotation marks omitted).

Thaler also notes that South Africa has granted patents with DABUS as an inventor. This foreign patent office was not interpreting our Patent Act. Its determination does not alter our conclusion.

We have considered Thaler’s additional arguments and find they do not merit discussion.

IV

When a statute unambiguously and directly answers the question before us, our analysis does not stray beyond the plain text. Here, Congress has determined that only a natural person can be an inventor, so AI cannot be. Accordingly, the decision of the district court is affirmed.

AFFIRMED

*1214 Costs

Costs shall be assessed against Appellant.

All Citations

43 F.4th 1207

Footnotes

- 1 The administrative records for both applications are materially identical.
- 2 While inventorship involves underlying questions of fact, see [Dana-Farber Cancer Inst., Inc. v. Ono Pharm. Co.](#), 964 F.3d 1365, 1370 (Fed. Cir. 2020), *cert. denied*, — U.S. —, 141 S. Ct. 2691, 210 L.Ed.2d 845 (2021), for purposes of this litigation the PTO has not challenged Thaler's representations, see D. Ct. Dkt. No. 25, at 11. Accordingly, our analysis must be consistent with the undisputed facts in the administrative record, drawing inferences in favor of the non-moving party. See [Safeguard Base Operations, LLC v. United States](#), 989 F.3d 1326, 1349 (Fed. Cir. 2021) (discussing when it is appropriate to supplement administrative record and noting "[t]he focal point for judicial review should be the administrative record already in existence") (quoting [Camp v. Pitts](#), 411 U.S. 138, 142, 93 S.Ct. 1241, 36 L.Ed.2d 106 (1973)).
- 3 The District Court had jurisdiction under [28 U.S.C. § 1331](#). See also [5 U.S.C. § 702](#) ("A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof.").
- 4 While [Mohamad](#) interpreted a statute other than the Patent Act, the Court's reasoning is directly applicable here. See generally [Legal Def. Fund v. Dep't of Agric.](#), 933 F.3d 1088, 1093-94 (9th Cir. 2019) (concluding that "individual" refers to human beings and not animals, based in part on [Mohamad](#)).
- 5 While the PTO also initially relied on the use of "whoever" in § 101 of the Patent Act, the PTO has also consistently explained that "individual" is limited to natural persons, a position we now uphold.

End of Document

© 2026 Thomson Reuters. No claim to original U.S. Government Works.