FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of

Thomson Reuters Corporation, a corporation, also d/b/a Thomson Reuters;

West Publishing Corporation, a corporation, also d/b/a West Publishing; and

Pondera Solutions, LLC, a limited liability company, also d/b/a Pondera Solutions, also d/b/a Pondera.

Complaint and Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center (EPIC)[1]

I. Summary

1. This complaint concerns the development, sale, and operation of an automated fraud detection system known primarily as "Fraud Detect"[2] by the Thomson Reuters Corporation and its subsidiaries, West Publishing Corporation and Pondera Solutions, LLC (collectively, "Thomson Reuters"). Thomson Reuters purports to accurately detect public benefits fraud through an opaque, proprietary algorithm and commercial data derived from sources like social media, credit reports, and housing records.[3] The company has continued to market and

[1] EPIC would like to thank two law clerks, Kabbas Azhar and Katrina Zhu, for their contributions to an earlier version of this complaint.

[2] Contracts for this product and Thomson Reuters' website describes this product using a variety of terms, including "FraudCaster," "Fraud Detect," "ID Risk Analytics," and "Fraud Detection as a Service." While Thomson Reuters lists Fraud Detect and ID Risk Analytics as separate product offerings on its website, EPIC believes that the underlying system for both offerings—derived from Pondera Solution's FraudCaster system—is the same. *See Improve Fraud Detection and Prevention with Fraud Detect*, Thomson Reuters, https://perma.cc/CH47-VTEX; *Detect, Prevent, and Mitigate Fraud in Your Program with ID Risk Analytics*, Thomson Reuters, https://perma.cc/T2J5-LPT2; Contract Amend. between the Ind. Fam. & Soc. Servs. Admin. and West Publishing Corporation 1 (Aug. 2, 2022), https://epic.org/wp-content/uploads/2023/11/Ind.-FSSA-Fraudcaster-Contract-Amendment-8.2.22.pdf; Press Release, Thomson Reuters, Thomson Reuters Announces ID Risk Analytics to Fight Government Fraud (Apr. 7, 2021), https://perma.cc/A5GV-HSRT.

[3] *See* D.C. Dep't of Hum. Servs., Pondera Proposal 7 (2020), https://perma.cc/9SCU-GSFW [hereinafter "D.C. Pondera Proposal"]; D.C. Dep't of Hum. Servs., Pondera Master Design Document 4–7, 10 (2021), https://perma.cc/28C6-2NJF [hereinafter "Pondera Master Design Document"]

offer its Fraud Detect product to state agencies and private healthcare companies across the country despite evidence that Thomson Reuters' fraud determinations are more often than not incorrect, leaving hundreds of thousands of legitimate claimants without access to public benefits.[4] Thomson Reuters has also failed to show that its Fraud Detect product meets accepted standards for responsible automated decision-making systems, such as those set out in Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of AI[5] and the White House's Blueprint for an AI Bill of Rights.[6]

2. Thomson Reuters has engaged in unfair and deceptive trade practices, both directly and by providing the means and instrumentalities for unfair and deceptive trade practices, in violation of Section 5 of the Federal Trade Commission Act ("FTC Act").[7] The company has also violated at least Sections 605, 607(b), 607(c), 607(d), and 611 of the Fair Credit Reporting Act ("FCRA")[8]—provisions that the Federal Trade Commission ("FTC" or "Commission") is empowered to enforce.[9]

3. For the reasons set out below, the Commission should open an investigation, secure an injunction against the offending business practices, seek model deletion or destruction of the Fraud Detect system,[10] and provide such other relief as the Commission deems necessary and appropriate.

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has played a leading role in developing FTC authority to address emerging privacy issues and to safeguard the privacy rights of consumers.[11] EPIC is also a

---

[4] *See, e.g.*, Cal. Leg. Analyst's Off., Assessing Proposals to Address Unemployment Insurance Fraud (2022), https://perma.cc/98SC-LGYH (finding that ID Risk Analytics incorrectly flagged 600,000 legitimate claimants as fraudulent, leading to unjust benefits suspension. This report places ID Risk Analytics' accuracy rate at 46%.).
[5] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (Oct. 30, 2023) [hereinafter "Executive Order 14110"].
[6] White House Off. Sci. & Tech. Pol'y, Blueprint for an AI Bill of Rights (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[7] 15 U.S.C. § 45.
[8] 15 U.S.C. §§ 1681c, 1681e, 1681g, 1681h, 1681i, 1681m, 1681s.
[9] 15 U.S.C. § 1681s.
[10] *See, e.g.*, Administrative Decision and Order at 6–7, *In re Rite Aid Corp.*, FTC File No. 072-3121 (2023) [hereinafter "Rite Aid Order"]; Jevan Hutson & Ben Winters, *America's Next "Stop Model!": Model Disgorgement* 14–16 (Priv. L. Scholars Conf. Working Paper, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225003.
[11] *See, e.g.*, EPIC, Comments on FTC Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (advanced notice issued Aug. 22, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; Consumer Reps. & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/ [hereinafter "EPIC FTC Commercial Surveillance Comment"]; EPIC, Comments on Proposed Consent Order, *In re Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (Oct. 8, 2021), https://archive.epic.org/apa/comments/In-re-SpyFone-Order-EPIC-comment-100821.pdf; EPIC et al., Comments on Proposed Consent Order, *In re Zoom Video Communications, Inc.*, FTC File

longstanding advocate for the transparent, ethical, and responsible development, procurement, and use of algorithms and artificial intelligence.[12]

5. Thomson Reuters is a Canadian media conglomerate, data broker, and information services providers with headquarters located at 19 Duncan Street, Ontario M5H 3H1, Canada.[13] Thomson Reuters, through subsidiaries including West Publishing Corporation[14] ("West Publishing") and Pondera Solutions, LLC.[15] ("Pondera"), markets a variety of algorithmic and automated risk analytics products to various healthcare, unemployment, and social services entities in the United States.[16] One of these risk products is the comprehensive fraud detection software variably named "FraudCaster," "Fraud Detect," "ID Risk Analytics," and "Fraud Detection as a Service."[17]

6. The FTC is an independent agency of the United States government given statutory authority and responsibility by, *inter alia*, the FTC Act, 15 U.S.C. §§ 41–58. The Commission is charged, *inter alia*, with enforcing section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which

---

No. 192-3167 (Dec. 14, 2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; EPIC, Comments on Proposed Consent Order, *In re Unrollme, Inc.*, FTC File No. 172-3139 (Sept. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; EPIC, Comments on Proposed Consent Agreements, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (Sept. 3, 2019), https://epic.org/apa/comments/EPIC-FTC-CambridgeAnalytica-Sept2019.pdf; EPIC, Comments on FTC Rule Setting Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (proposed Apr. 4, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf; EPIC, Comments on Proposed Consent Order, *In re Uber Technologies, Inc.*, FTC File No. 152-3054 (May 14, 2018), https://epic.org/apa/comments/EPIC-FTC-Revised-Uber-Settlement.pdf; EPIC, Comments on Proposed Consent Order, *In re Paypal, Inc.*, FTC File No. 162-3102 (Mar. 29, 2018), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Google Inc.* (July 31, 2017), https://www.epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf; Complaint and Request for Investigation, Injunction, and Other Relief, *In re Genesis Toys and Nuance Communications* (Dec. 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

[12] *See, e.g.*, EPIC, Outsourced & Automated: How AI Companies Have Taken Over Government Decision-Making (Sept. 14, 2023), https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-w-Appendix-Updated-9.26.23.pdf [hereinafter "Outsourced & Automated Report"]; EPIC, Comments on Notice of Proposed Rulemaking, *In re Access to Video Conferencing*, CG Docket No. 23-161 (Sept. 6, 2023), https://epic.org/documents/in-re-access-to-video-conferencing/; EPIC, Comments on Proposed Parental Consent Method Submitted by Yoti, Inc., Under the Voluntary Approval Processes Provisions of the Children's Online Privacy Protection Rule, 88 Fed. Reg. 46705 (Aug. 21, 2023), https://epic.org/documents/epic-cdd-fairplay-comments-to-the-ftc-on-proposed-parental-consent-method-submitted-by-yoti-inc-under-coppa-rule/; EPIC, Generating Harms: Generative AI's Impact & Paths Forward (May 23, 2023), https://epic.org/gai.

[13] *Office Locations*, Thomson Reuters, https://perma.cc/B5P6-LTTZ.

[14] *Vendor Information for West Publishing Corporation*, Thomson Reuters, https://perma.cc/9R8W-KGWC.

[15] *See* Press Release, Thomson Reuters, Thomson Reuters Acquires Pondera Solutions (Mar. 19, 2020), https://perma.cc/7MRG-QPCF.

[16] *See Detect, Prevent, and Mitigate Fraud in Your Program with ID Risk Analytics*, Thomson Reuters, https://perma.cc/T2J5-LPT2; Press Release, Thomson Reuters, Thomson Reuters Announces ID Risk Analytics to Fight Government Fraud (Apr. 7, 2021), https://perma.cc/A5GV-HSRT; Contract Between Il. Dep't Emp. Sec. and Pondera Solutions 4, https://perma.cc/NQ8M-9QPA; *Improve Fraud Detection and Prevention with Fraud Detect*, Thomson Reuters, https://perma.cc/CH47-VTEX.

[17] *Id.*

prohibits unfair and deceptive acts or practices in or affecting commerce, including violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681s.

III. Established Public Policies for the Use of Artificial Intelligence

A. The OECD AI Principles

7. In 2019, the member nations of the Organization for Economic Cooperation and Development ("OECD"), including the United States,[18] promulgated the OECD Principles on Artificial Intelligence.[19] The United States has expressly endorsed the OECD Principles.[20]

8. According to the OECD AI Principle on Human-Centered Values and Fairness, "AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity, and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognized labour rights."[21]

9. According to the OECD AI Principle on Transparency and Explainability, AI actors should "provide meaningful information, appropriate to the context, and consistent with the state of art (i) to foster a general understanding of AI systems, (ii) to make stakeholders aware of their interactions with AI systems, including in the workplace, (iii) to enable those affected by an AI system to understand the outcome, and (iv) to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."[22]

10. According to the OECD AI Principle on Robustness, Security, and Safety, "AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk."[23]

11. According to the OECD AI Principle on Accountability, "[o]rganisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles."[24]

12. The OECD Principles on Artificial Intelligence are "established public policies" within the meaning of the FTC Act.[25]

---

[18] *Timeline*, OECD, https://www.oecd.org/60-years/timeline/ (last visited Dec. 18, 2023).
[19] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[20] Press Release, Fiona Alexander, NTIA, U.S. Joins with OECD in Adopting Global AI Principles (May 22, 2019), https://www.ntia.gov/blog/us-joins-oecd-adopting-global-ai-principles.
[21] OECD Principle 1.2(a), *supra* note 19.
[22] OECD Principle 1.3, *supra* note 19.
[23] OECD Principle 1.4(a), *supra* note 19.
[24] OECD Principle 1.5, *supra* note 19.
[25] 15 U.S.C. § 45(n).

B. The Blueprint for an AI Bill of Rights

24. On October 4, 2022, the White House Office of Science and Technology Policy ("OSTP") published its Blueprint for an AI Bill of Rights, a set of principles meant to guide the development, deployment, and use of automated systems and protect the rights of the American public.[26] OSTP designed the Blueprint for an AI Bill of Rights to be "fully consistent" with public policies that govern the development, deployment, and use of AI—including the OECD AI Principles.[27]

25. According to the Blueprint's Principle of Safe and Effective Systems, AI and automated systems should "undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards."[28]

26. According to the Blueprint's Principle of Algorithmic Discrimination Protections, "designers, developers, and deployers of automated systems should take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way. This protection should include proactive equity assessments as part of the system design, use of representative data and protection against proxies for demographic features, ensuring accessibility or people with disabilities in design and development, pre-deployment and ongoing disparity testing and mitigation, and clear organizational oversight."[29]

27. According to the Blueprint's Principle of Notice and Explanation, "designers, developers, and deployers of automated systems should provide generally accessible plain language documentation including clear descriptions of the overall system functioning and the role automation plays, notice that such systems are in use, the individual or organization responsible for the system, and explanations of outcomes that are clear, timely, and accessible. Such notice should be kept up-to-date, and people impacted by the system should be notified of significant use case or key functionality changes."[30]

28. According to the Blueprint's Principle of Human Alternatives, Consideration, and Fallback, "automated systems with an intended use within sensitive domains, including, but not limited to, criminal justice, employment, education, and health, should additionally be tailored to the purpose, provide meaningful access for oversight, include training for nay people interacting with the system, and incorporation human consideration for adverse or high-risk decisions."[31]

---

[26] *What is the Blueprint for an AI Bill of Rights?*, OSTP (Oct. 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/.
[27] *See Relationship to Existing Law and Policy*, OSTP (Oct. 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/relationship-to-existing-law-and-policy/.
[28] OSTP, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People 5 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
[29] *Id.*
[30] *Id.* at 6.
[31] *Id.* at 7.

29. The principles outlined by OSTP's Blueprint for an AI Bill of Rights are "established public policies" within the meaning of the FTC Act.[32]

C. NIST AI Risk Management Framework

30. On January 26, 2023, the National Institute of Standards and Technology ("NIST") published its AI Risk Management Framework ("AI RMF"), alongside various companion resources.[33] The AI RMF is "designed to equip organizations and individuals… with approaches that increase the trustworthiness of AI systems, and to help foster the responsible design, development, deployment, and use of AI systems over time."[34] It is "intended to be practical, to adapt to the AI landscape as AI technologies continue to develop, and to be operationalized by organizations in varying degrees and capacities so society can benefit from AI while also being protected from its potential harms."[35]

31. Under Section 5.1 of the AI RMF, NIST states that AI risk management processes and outcomes should be "established through transparent policies, procedures, and other controls based on organizational risk priorities" and that "organizational policies and practices [should be] in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts."[36]

32. Section 5.1 of the AI RMF also recommends that "organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly."[37]

33. Under Section 5.2 of the AI RMF, NIST states that organizations developing, selling, or using AI should examine and document the "potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness."[38]

34. Under Section 5.3 of the AI RMF, NIST states that (1) "AI system performance or assurance criteria [should be] measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s)," (2) "the functionality and behavior of the AI system and its components… [should be] monitored when in production," (3) "the AI system to be deployed [should be] demonstrated to be valid and reliable," (4) "the AI system [should be] evaluated regularly for safety risks," and (5) "[AI system] fairness and bias… [should be] evaluated and results [should be] documents."[39]

---

[32] 15 U.S.C. § 45(n).
[33] *See* Nat'l Inst. Standards & Tech., Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[34] *Id.* at 2.
[35] *Id.* at 2.
[36] *Id.* at 22–23.
[37] *Id.* at 24.
[38] *Id.* at 27.
[39] *Id.* at 29–30.

35. Under Section 5.4 of the AI RMF, NIST recommends that (1) AI organizations should follow "procedures… to respond to and recover from a previously unknown risk when it is identified," (2) "mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use," (3) "post-deployment deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management," and (4) "incidents and errors are communicated to relevant AI actors, including affected communities."[40]

36. NIST's AI RMF is an "established public policy" within the meaning of the FTC Act.[41]

D. Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of AI

37. On October 30, 2023, the White House published Executive Order 14110, setting out comprehensive guidelines to manage the development, procurement, and use of AI.[42] These guidelines include both restrictions on how federal agencies develop, procure, and use AI technologies and provisions encouraging responsible private-sector development and deployment of AI through federal funding restrictions and federal agency enforcement priorities.[43]

38. Under Section 5.3 of Executive Order 14110, the White House encourages the FTC to "consider, as it deems appropriate, whether to exercise the Commission's existing authorities, including its rulemaking authority under the Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*, to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI."[44]

39. Section 2 of Executive Order 14110 sets out eight guiding principles and priorities concerning responsible AI development and use. These policy priorities include:

    a. Ensuring that AI is safe and secure through "robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use";[45]

    b. Ensuring that AI policies are consistent with the White House's dedication to advancing equity and civil rights, including efforts to combat the "use of AI to disadvantage those who are already too often denied equal opportunity and justice"[46]

[40] *Id.* at 32–33.
[41] 15 U.S.C. § 45(n).
[42] Executive Order 14110.
[43] *See id.* at 75196–98, 75204–05, 75209–75218.
[44] *Id.* at 75209.
[45] *Id.* at 75191.
[46] *Id.* at 75192.

and to "hold those developing and deploying AI accountable to standards that protect against unlawful discrimination and abuse";[47]

c. Protecting the "interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives," including efforts to "enforce existing consumer protection laws and principles and enact appropriate safeguards against fraud, unintended bias, discrimination, infringements on privacy, and other harms of AI";[48] and

d. Protecting "American's privacy and civil liberties," including efforts to "ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks."[49]

40. Executive Order 14110 builds on earlier White House policies on responsible AI development and use, including the OSTP's Blueprint for an AI Bill of Rights and the NIST AI RMF.[50]

41. Executive Order 14110 is an "established public policy" within the meaning of the FTC Act.[51]

IV. Factual Background

A. Thomson Reuters' Fraud Detect Purports to Detect and Prevent Public Benefits Fraud Using Proprietary Algorithms and Thomson Reuters' CLEAR Database

42. On March 19, 2020, amid the global COVID-19 pandemic that severely stressed public benefits programs around the country,[52] Thomson Reuters acquired Pondera Solutions, the company behind the automated fraud detection and prevention system known as FraudCaster.[53] In its acquisition announcement, Thomson Reuters claimed that "Pondera Solutions leverages advanced analytics, AI, and human intelligence to help government and commercial healthcare programs maintain compliance and detect fraud, waste, and abuse.

[47] *Id.*
[48] *Id.*
[49] *Id.* at 75193.
[50] *Id.* at 75192.
[51] 15 U.S.C. § 45(n).
[52] *See, e.g.*, Drew DeSilver, *What the Data Says About Food Stamps in the U.S.*, Pew Rsch. Ctr (July 19, 2023), https://www.pewresearch.org/short-reads/2023/07/19/what-the-data-says-about-food-stamps-in-the-u-s/; Ctr. on Budget & Pol'y Priorities, The Covid-19 Economy's Effects on Food, Housing, and Employment Hardships (Feb. 10, 2022), https://www.cbpp.org/sites/default/files/8-13-20pov.pdf; Rakesh Kochhar, *Unemployment Rose Higher in Three Months of COVID-19 Than It Did in Two Years of the Great Recession*, Pew Rsch. Ctr. (June 11, 2020), https://www.pewresearch.org/short-reads/2020/06/11/unemployment-rose-higher-in-three-months-of-covid-19-than-it-did-in-two-years-of-the-great-recession/. Similar stressors are returning as agencies begin to phase out dedicated COVID-19 benefits programs. *See* Ashraf Khalil, *Many Americans Facing Hardship as Benefits Created During COVID-19 End*, PBS News Hour (May 11, 2023), https://www.pbs.org/newshour/nation/many-americans-facing-hardship-as-benefits-created-during-covid-19-end.
[53] Press Release, Thomson Reuters, Thomson Reuters Acquires Pondera Solutions (Mar. 19, 2020), https://perma.cc/7MRG-QPCF.

Their core detection system, FraudCaster, helps clients detect and prevent hundreds of millions of dollars in improper payments in health plans and government programs."[54]

43. According to Thomson Reuters' webpage on Fraud Detect, the fraud detection system is designed to meet "industry-specific needs" for managing the allocation of public benefits like unemployment insurance and Supplemental Nutrition Assistance Program (SNAP) funds by, e.g., vetting benefits applicants and identifying overpayments for debt collection proceedings.[55] On the same page that it markets Fraud Detect to public benefits agencies, Thomson Reuters disclaims all liability under the Fair Credit Reporting Act (FCRA) by stating that Fraud Detect "may not be used as a factor in consumer debt collection decisioning; establishing a consumer's eligibility for credit, insurance, employment, government benefits, or housing; or for any other purpose authorized under the FCRA."[56]

44. In its contract proposal to the D.C. Department of Human Services, Pondera claimed that FraudCaster would be a "force multiplier" for the agency in the face of "limited resources and a constant influx of new referrals" by helping the agency "understand recipient and retailer risk," "identify prior behaviors and patterns of fraudulent behavior," and ensure the "assignment and prioritization of the true highest value cases."[57]

45. After Pondera's acquisition, Thomson Reuters integrated its CLEAR investigation platform into the FraudCaster product.[58] The CLEAR platform, a searchable database of billions of public and proprietary commercial records from over 60 data sources,[59] is at the core of many of Thomson Reuters' fraud detection services and marketed as a fraud mitigation system for, e.g., tax agencies,[60] healthcare companies,[61] and insurance companies.[62] The CLEAR platform is also the subject of a class action lawsuit alleging that Thomson Reuters creates a "cradle-to-grave dossier" for each person in its database, which it sells to third parties.[63]

46. Thomson Reuters' CLEAR platform incorporates a wide array of consumer data and credit header data, including but not limited to individual and business records, identity information, criminal backgrounds, incarcerations, deceased status, best known address, affiliates, linkages, and social media information.[64] Many types of data found within the CLEAR platform—such as criminal background information and housing records—are

---

[54] *Id.*
[55] *Improve Fraud Detection and Prevention with Fraud Detect*, Thomson Reuters, https://perma.cc/CH47-VTEX.
[56] *Id.*
[57] D.C. Pondera Proposal at 7.
[58] *See, e.g.*, Pondera Master Design Document at 5–6; *cf. also Thomson Reuters CLEAR*, Thomson Reuters, https://perma.cc/7Y7Q-572S.
[59] *Id.*
[60] *See CLEAR for Tax and Revenue Agencies*, Thomson Reuters, https://perma.cc/8BE2-VFGF.
[61] *See CLEAR for Healthcare Fraud, Waste, and Abuse Investigations*, Thomson Reuters, https://perma.cc/U688-SVUL.
[62] *See CLEAR for Insurance Investigations*, Thomson Reuters, https://perma.cc/R74V-WRKQ.
[63] *See Thomson Reuters CLEAR Lawsuit*, Gibbs Law Group (2022), https://perma.cc/8JBN-6EXA.
[64] Pondera Master Design Document at 5.

regularly included within consumer reports[65] and have been linked to racially biased algorithmic outputs due to, *inter alia*, historical redlining practices and racial disparities in policing.[66]

47. After integrating its CLEAR database into Pondera's FraudCaster system, Thomson Reuters renamed the automated fraud detection system, "ID Risk Analytics."[67] In some state government contracts—and Thomson Reuters' website[68]—Thomson Reuters or one of its subsidiaries instead refers to its automated fraud detection offering as "Fraud Detect"[69] or "Fraud Detection as a Service."[70] In other states like Nevada, Thomson Reuters may provide a state-branded version of its automated fraud detection system.[71] For ease of reference, this complaint uses the umbrella term "Fraud Detect" to encompass Pondera's FraudCaster system, Thomson Reuters' Fraud Detect system, and Thomson Reuters' ID Risk Analytics system, all of which appear to use the same automated fraud detection system.

48. Thomson Reuters' Fraud Detect system uses a combination of historical public benefits program data and proprietary commercial data about recipients to train rule-based algorithms that it claims can predict "fraud or other collusive activities."[72]

49. To make these predictions, Thomson Reuters compiles sensitive data about public benefits recipients and retailers from both government and third-party, commercial data sources.[73] The data points that Thomson Reuters compiles and uses for fraud predictions include, *inter alia*, recipients' home addresses, how far recipients travel to buy groceries, affiliated persons, and social media profiles.[74]

---

[65] *See* 15 U.S.C. § 1681c. This data also includes "credit header data." *See* FTC, *Individual Reference Services – A Report to Congress* (1997) ("A 'credit header' is the portion of a credit report that typically contains an individual's name, aliases, birth date, Social Security number, current and prior addresses, and telephone number.").
[66] *See generally* Anya E. R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020), https://perma.cc/SC2T-8RHN; Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018).
[67] Press Release, Thomson Reuters, Thomson Reuters Announces ID Risk Analytics to Fight Government Fraud (Apr. 7, 2021), https://perma.cc/A5GV-HSRT; *cf. also Improve Fraud Detection and Prevention with Fraud Detect*, Thomson Reuters, https://perma.cc/CH47-VTEX; *See the Power of Advanced Fraud Analytics and Machine Learning*, Thomson Reuters, https://perma.cc/5GS3-5CDM.
[68] The product presented on Thomson Reuters' product page for ID Risk Analytics is a Fraud Detect module. *See Detect, Prevent, and Mitigate Fraud in Your Program with ID Risk Analytics*, Thomson Reuters, https://perma.cc/T2J5-LPT2.
[69] *See, e.g.*, Contract Amend. between the Ind. Fam. & Soc. Servs. Admin. and West Publishing Corporation 1 (Aug. 2, 2022), https://epic.org/wp-content/uploads/2023/11/Ind.-FSSA-Fraudcaster-Contract-Amendment-8.2.22.pdf
[70] *See, e.g.*, Contract between Iowa Dep't Pub. Health & Pondera Solutions 5, https://epic.org/wp-content/uploads/2023/10/FY19_Iowa_Service_Contract_Pondera_Solutions.pdf.
[71] *See, e.g.*, Contract between Nev. Dep't Health & Hum. Servs. & Pondera Solutions 13, https://epic.org/wp-content/uploads/2023/10/PonderaContract-FullyExecuted-1.pdf.
[72] *See* D.C. Pondera Proposal at 3, 7; Pondera Master Design Document at 5–6.
[73] *Fraud Detect*, Thomson Reuters, https://perma.cc/E585-C459; *see also* Contract between Ill. Dep't of Emp. Sec. & Pondera Solutions 57, https://perma.cc/NQ8M-9QPA; Contract between D.C. Dep't of Hum. Servs. & Pondera Solutions 14–15, https://perma.cc/56C7-WYB3.
[74] *See* D.C. Pondera Proposal at 8; Pondera Master Design Document at 5, 7, 10.

50. Thomson Reuters' Fraud Detect works by producing Alerts of "anomalous behavior and conditions that warrant further review" based on ongoing analyses of recipient data gleaned from government and third-party, commercial data sources.[75] Fraud Detect also generates Risk Scores and Scorecard rankings based on the "frequency and severity of alerts" regarding a recipient or others in their household.[76]

51. According to Thomson Reuters' webpage on ID Risk Analytics, Fraud Detect separates benefits fraud alerts into three priority tiers—"High Risk," "Medium Risk," and "Low Risk"—based on "applicant metrics and claim metrics," as well as seemingly disparate data points like "home addresses, phone numbers, and incarceration data."[77] As of January 2021, Fraud Detect instead separated its Alerts into five risk tiers. In order, these tiers were "1 – Potential for Fraud/Risk," "2 – Highly Suspect," "3 – Needs Review," "4 – Suspect Element," and "5 – Informational Data Point."[78] Specific applicant and claim metrics for fraud alerts included recipients entering into high-dollar-amount transactions, recipients traveling 25 miles or more to shop at a big box store, and recipients requesting their EBT card balance 12 or more times in a year.[79]

52. Fraud Detect's Scorecard allows agency customers to rank households based on fraud and overpayment risk. To produce these rankings, Fraud Detect generates a risk score (0-100) based on alerts and "other analytics and patterns."[80] Fraud Detect's risk scoring algorithm is "continually fine tune[d]" after deployment, so the accuracy of risk scores varies over time.[81]

53. Thomson Reuters' Fraud Detect also includes a SuperSearch feature, which allows customers to search through recipient data.[82] Through its SuperSearch Premium offering, Thomson Reuters also allows customers to search public records and social media data about public benefits recipients.[83]

B. Thomson Reuters Provides Its Fraud Detect System to Agencies Across the Country

41. Thomson Reuters provides its Fraud Detect system to government agencies in at least 42 states.[84] Many of these offerings come from cooperative purchasing agreements facilitated by portfolio companies like SHI International Corp. and intermediaries like NASPO

[75] Pondera Master Design Document at 4.
[76] *Id.* at 4–5.
[77] *Detect, Prevent, and Mitigate Fraud in Your Program with ID Risk Analytics*, Thomson Reuters, https://perma.cc/T2J5-LPT2.
[78] Pondera Master Design Document at 8.
[79] *Id.* at 9–11.
[80] *Id.* at 11.
[81] *Id.*
[82] *Id.* at 6–7.
[83] *Id.*
[84] *See* Outsourced & Automated Report at 14, 43, 72–143.

ValuePoint.[85] The total potential market value that Thomson Reuters derives from these contracts is at least $30,861,374—and potentially far higher.[86]

42. In several states—including Illinois,[87] Indiana,[88] Iowa,[89] and Nevada,[90] as well as the District of Columbia[91]—Thomson Reuters maintains and operates its Fraud Detect system on behalf of public benefits agencies. The alerts, risk scores, and fraud determinations that Thomson Reuters makes directly impact who continues to receive public benefits, whose benefits are revoked, and whose benefits are clawed back as alleged overpayments.[92]

C. Thomson Reuters' Fraud Detect Regularly Flags Legitimate Public Benefits Claims as Fraudulent, Leading to the Wrongful Reduction, Denial, and Recollection of Public Benefits for Eligible Recipients

43. Agencies across the country rely on Thomson Reuters' Fraud Detect to determine how much assistance public benefits recipients should receive, if any, as well as whether and when to initiate fraud investigations or overpayment proceedings.[93]

44. Although Thomson Reuters and Pondera have marketed Fraud Detect as an automated fraud detection and prediction system, they have included data points within Fraud Detect that relate to consumer debt instead of fraud indicators.[94] Fraud Detect has been used to claw back purported years-old improper overpayments from public benefits recipients who did not commit fraud, falsely flagging consumers as fraudsters when agency officials erred.[95]

45. Thomson Reuters' Fraud Detect is frequently incorrect in its fraud predictions, accusing legitimate benefits recipients of fraud. In December 2020, for example, California's

---

[85] *Id.*; *see also* SHI Int'l Corp., NASPO ValuePoint, SHI Current Product Catalog, https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/shi-international-corp/ (last visited Dec. 18, 2023) (document under Pricing Documents).
[86] This estimate comes from EPIC's own research into a sample of 621 state AI contracts around the country. *See* Outsourced & Automated Report at 37–39.
[87] *See* Contract between Ill. Dep't Emp. Sec. and Pondera Solutions 4, https://epic.org/wp-content/uploads/2023/10/Illinois-FraudCaster-Contract.pdf.
[88] *See* Contract between Ind. Dep't Workforce Dev. and Pondera Solutions 36–43, https://epic.org/wp-content/uploads/2023/10/Indiana-FraudCaster-Contract.pdf; Contract between Ind. Fam. & Soc. Servs. Admin. And West Publishing 2, https://epic.org/wp-content/uploads/2023/10/Indiana-FSSA-FraudCaster-Contract.pdf.
[89] *See* Contract between Iowa Dep't Pub. Health and Pondera Solutions 4–5, https://epic.org/wp-content/uploads/2023/10/Iowa-Pondera-Contract.pdf.
[90] *See, e.g.*, Contract between Nevada Dep't Health & Hum. Servs., Div. Welfare & Supportive Servs. and Pondera 13–19, https://epic.org/wp-content/uploads/2023/10/Nevada-Pondera-Contract.pdf.
[91] Contract between D.C. Dep't of Hum. Servs. & Pondera Solutions 11, https://perma.cc/56C7-WYB3.
[92] *See, e.g.*, EPIC, Screened & Scored in the District of Columbia 25 (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf [hereinafter "Screened & Scored Report"]; David Lightman, *California's Effort to Fight Unemployment Fraud Hurt Many Deserving Recipients, Report Finds*, Sacramento Bee (Feb. 18, 2022), https://www.sacbee.com/news/politics-government/capitol-alert/article258505593.html (California stopping payment of all fraud claims marked as suspicious by Pondera).
[93] *See id.;* Outsourced & Automated Report at 43, 68–123.
[94] *See* Screened & Scored Report at 25; Contract between Nevada Dep't Health & Hum. Servs., Div. Welfare & Supportive Servs. and Pondera 15–16, https://epic.org/wp-content/uploads/2023/10/Nevada-Pondera-Contract.pdf.
[95] *Id.*; *see also* Virginia Eubanks, *Zombie Debts Are Hounding Struggling Americans. Will You Be Next?*, Guardian (Oct. 15, 2019), https://perma.cc/92TW-7AK5.

Employment Development Department hired Pondera to review 10 million unemployment insurance claims paid out since the beginning of the COVID-19 pandemic.[96] Pondera flagged 1.1 million claims as "suspicious," and all 1.1 million claimants' benefits were suspended. Further investigation showed that more than 600,000 (54%) of the claims flagged by Pondera as fraudulent were actually legitimate.[97]

46. Under other contracts, Thomson Reuters' Fraud Detect has been used explicitly to identify and pursue overpayments instead of detecting and preventing fraud. For example, in 2014, the Iowa Workforce Development ("IWD") agency contracted with Pondera Solutions for its FraudCaster system, purportedly to detect and combat fraud,[98] but a subsequent open records request submitted by 2022 EPIC Scholar-in-Residence Virginia Eubanks revealed that IWD was using FraudCaster to identify and pursue unemployment benefit overpayment collections.[99]

47. Within its contract with IWD, Pondera characterized the mere presence of improper payments as fraud, even without other indicators of fraud.[100] In practice, FraudCaster's improper payment determinations subjected Iowa residents who were eligible for unemployment benefits to false fraud allegations and improper debt collection proceedings.[101]

48. In 2018, for example, Iowa resident Andrew Dorliae was fired from his job at Whirlpool Corporation and applied for unemployment benefits. IWD initially determined that Dorliae was eligible, but after his employer challenged Dorliae's eligibility, IWD reversed their eligibility determination and used FraudCaster to initiate an overpayment proceeding; Dorliae was flagged for fraud and threatened with debt collection proceedings if he did not voluntarily repay the funds he received as unemployment benefits. After appealing "every decision [IWD] made," IWD eventually reaffirmed his eligibility for unemployment benefits.[102]

49. For other Iowa residents like Kevin Christopherson, the burden of successive administrative appeals on top of unemployment stressors meant that eligibility reversals and overpayment determinations made by IWD under the Pondera contract—even erroneous determinations—often remained unchallenged.[103]

---

[96] *See* Lightman, *supra* note 92.
[97] *Id.*; *see also* Cal. Leg. Analyst's Off., *supra* note 4 (finding that Thomson Reuters' Fraud Detect incorrectly flagged 600,000 legitimate claimants as fraudulent, leading to unjust benefits suspension. This finding places Fraud Detect's accuracy rate at 46%.).
[98] *See* Mark Anderson, *Pondera Solutions Works with Iowa Employment Agency*, Sacramento Bus. J. (Apr. 3, 2014), https://www.bizjournals.com/sacramento/news/2014/04/03/pondera-works-with-iowa-employment-agency.html.
[99] *See* Eubanks, *supra* note 95.
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*

D. Thomson Reuters Has Withheld Key Information Concerning the Design, Evaluation, and Operation of Fraud Detect from Government Agencies and the General Public

50. Under many of its contracts with state agencies, Thomson Reuters maintains control and ownership over the Fraud Detect system, including control over the source code, operation, and maintenance of Fraud Detect.[104]

51. EPIC has attempted to access information concerning the design, evaluation, and operation of Fraud Detect from government agencies using open records laws, but multiple agencies have stated that they either do not have access to the information or cannot disclose it due to trade secret restrictions. For example, in response to a 2021 open records request filed by EPIC, the Illinois Department of Employment Security withheld several documents on the grounds that they were "proprietary and confidential" information exempted from disclosure under open records laws.[105]

52. EPIC has also attempted to access information pertaining to the Fraud Detect system's accuracy and reliability, only to find that Thomson Reuters offered no such information to government agencies. For example, in another 2021 open records request filed by EPIC, the District of Columbia's Department of Human Services revealed that it had no documents pertaining to accuracy testing for the Fraud Detect system, nor any information on how its contract with Thomson Reuters has impacted public benefits recipients within the District of Columbia.[106]

53. Former Pondera CEO and current Thomson Reuters Vice President Jon Coss has stated that companies like Thomson Reuters intentionally withhold information about the logic and operation of automated systems like Fraud Detect from agencies and the public to thwart fraudsters and "bad guys."[107]

54. As a result of Thomson Reuters' secrecy, public benefits recipients, government agencies, legal aid organizations, and civil society organizations like EPIC do not have access to key information necessary to identify and redress consumer harms caused by Fraud Detect. These consumer harms may include false fraud allegations,[108] wrongful denials or terminations of

---

[104] *See, e.g.*, Contract between Ill. Dep't Emp. Sec. and Pondera Solutions 45–49, https://epic.org/wp-content/uploads/2023/10/Illinois-FraudCaster-Contract.pdf; Contract between Nevada Dep't Health & Hum. Servs., Div. Welfare & Supportive Servs. and Pondera 13–17, https://epic.org/wp-content/uploads/2023/10/Nevada-Pondera-Contract.pdf.

[105] Outsourced & Automated Report at 22; *see also* Virginia Eubanks, *Item 10: How a Small Legal Aid Team Took on Algorithmic Black Boxing at Their State's Employment Agency (and Won)*, EPIC (Dec. 1, 2022), https://epic.org/item-10/ (detailing hurdles for accessing similar information in Arkansas).

[106] *See* Screened & Scored Report at 24.

[107] Thomson Reuters, *Follow the Money: Fighting Fraud in the Unemployment Insurance System During COVID-19*, https://perma.cc/BYR6-M7XA; *see also* Jon Coss, *Catching Bad Guys: Preventing and Combating Fraud in Government Programs*, Thomson Reuters, https://perma.cc/Y3W9-ZB5J.

[108] Lightman, *supra* note 92; *see also Michigan Unemployment Insurance False Fraud Determinations*, Benefits Tech. Advoc. Hub, https://www.btah.org/case-study/michigan-unemployment-insurance-false-fraud-determinations.html (last visited Dec. 18, 2023).

public benefits for eligible recipients,[109] wrongful benefits overpayment collections and similar improper debt proceedings,[110] consumer privacy violations due to the improper use and transfer of sensitive personal information,[111] and algorithmic discrimination.[112]

V. Legal Analysis

A. The Federal Trade Commission Act

50. Section 5 of the Federal Trade Commission Act (FTC Act) prohibits unfair and deceptive acts and practices.[113]

51. A company engages in an unfair trade practice if the "act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[114] The Commission may consider established public policies along with other evidence.[115]

52. Deceptive acts and practices include material representations, omissions, or practices that are likely to mislead a consumer acting reasonably in the circumstances.[116]

53. The Commission has stated that a company also violates Section 5 of the FTC Act when it furnishes others with the means and instrumentalities for the commission of unfair and deceptive acts and practices.[117]

---

[109] *Id.*; *see also* Eubanks, *supra* note 95; Grant Fergusson, *Public Benefits, Privacy Vendors: How Private Companies Help Run our Welfare Programs*, EPIC (Jan. 26, 2023), https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/.
[110] *See* Screened & Scored Report at 25; Eubanks, *supra* note 95.
[111] *See* Outsourced & Automated Report at 11–16; Fergusson, *supra* note 109; *cf.* EPIC FTC Commercial Surveillance Comment at 30–108 (describing exploitative commercial data practices and how automated decision-making systems facilitate further privacy harms).
[112] *See* Outsourced & Automated Report at 17–21; *cf.* EPIC FTC Commercial Surveillance Comment at 68–75 (discussing several ways that bias can be injected into automated decision-making).
[113] 15 U.S.C. § 45.
[114] 15 U.S.C. § 45(n); *see also* FTC, Policy Statement on Unfairness (1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [hereinafter "FTC Unfairness Policy Statement"].
[115] *Id.*
[116] FTC, Policy Statement on Deception (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[117] Complaint at 41, *FTC v. Neora, LLC, Signum Biosciences, Inc., Signum Nutralogix, Jeffrey Olson, Maxwell Stock, and Jeffry Stock*, FTC File No. 162-3099 (2019), https://www.ftc.gov/system/files/documents/cases/1623099_nerium_complaint_11-1-19.pdf (deceptive acts or practices); *see also* Complaint at 24, *FTC v. Office Depot, Inc., and Support.com, Inc.*, FTC File No. 172-3023 (2019), https://www.ftc.gov/system/files/documents/cases/office_depot_complaint_3-27-19.pdf (deceptive acts or practices); Complaint at 7, *In re DesignerWare, LLC*, FTC File No. 112-3151 (2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf (unfair acts or practices); Complaint at 10–11, *FTC v. CyberSpy Software, LLC, and Trace R. Spence*, No. 08-cv-01872, 2008 WL 5157718 (M.D. Fl. Nov. 5, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf (unfair acts or practices).

B. The Fair Credit Reporting Act

54. The Fair Credit Reporting Act (FCRA) governs the collection and use of consumer report information and regulates the practices of consumer reporting agencies (CRAs), which collect and compile consumer information for use in establishing a consumer's eligibility for credit, insurance, employment, licensure, or "other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status."[118]

55. Section 621 of FCRA authorizes the FTC to enforce compliance with the Act using its authority under Section 5(a) of the FTC Act.[119] For the purposes of FTC enforcement, all FCRA violations "shall constitute an unfair or deceptive act or practice in commerce, in violation of section 5(a) of the Federal Trade Commission Act."[120]

56. The FTC has stated that FCRA was enacted with three goals in mind: (a) to prevent the misuse of sensitive consumer information by limiting recipients to those who have a legitimate need for it; (b) to improve the accuracy and integrity of consumer reports; and (c) to promote the efficiency of the nation's banking and consumer credit systems.[121]

57. To meet these goals, FCRA defines both consumer reports and CRAs broadly. With a few exceptions, a "consumer report" is defined as a communication of information by a CRA bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for, *inter alia*, credit, employment, or public benefits.[122] A CRA is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."[123]

58. Under Section 605 of FCRA, CRAs are generally prohibited from making consumer reports containing information about, *inter alia*:

    a. civil suits, civil judgments, and records that antedate the report by more than seven years or that have passed their relevant statute of limitations;

---

[118] 15 U.S.C. § 1681b; *see also* FTC, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations 1 (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf [hereinafter "2011 FTC Staff Summary"].
[119] 15 U.S.C. § 1681s.
[120] *Id.*
[121] 2011 FTC Staff Summary at 1.
[122] 15 U.S.C. § 1681a(d).
[123] 15 U.S.C. § 1681a(f).

b. accounts placed for collection or charged to profit and loss that antedate the report by more than seven years; and

c. "any other adverse item of information, other than records of convictions of crimes[,] which antedates the report by more than seven years."[124]

59. Under Section 607(b) of FCRA, CRAs are required, when generating a consumer report about an individual, to "follow reasonable procedures to assume maximum possible accuracy of the information concerning the individual about whom the report relates."[125] On October 20, 2022, the Consumer Financial Protection Bureau issued an advisory opinion clarifying that consumer reporting agencies needed to maintain procedures capable of preventing the inclusion of facially false data like "logical inconsistencies relating to consumer data and/or the status or other information associated with consumer accounts."[126] For example, facially false data includes "information about consumer accounts that is plainly inconsistent with other reported information," such as one source claiming the consumer is deceased while other sources report ongoing payment activity.[127]

60. Section 607(c) of FCRA requires CRAs to permit disclosure of the contents of a consumer report to a consumer if the report was used to make an adverse action against the consumer.[128]

61. Section 607(d) of FCRA requires CRAs to provide a notice to any person who receives a consumer report detailing their responsibilities under the Act.[129]

62. If a consumer disputes the completeness or accuracy of any information contained within the consumer's file maintained by a CRA, Section 611 of FCRA requires the CRA to, "free of charge, conduct a reasonable reinvestigation to determine whether disputed information is inaccurate and record the current status of the disputed information, or [promptly] delete the item from the [consumer's] file… before the end of the 30-day period beginning on the date on which the agency receives the notice of the dispute from the consumer or reseller."[130] CRAs must also provide notification of the dispute to "any person who provided any item of information in dispute" within five days after receiving notice of a dispute from a consumer or reseller.[131]

[124] 15 U.S.C. § 1681c.
[125] 15 U.S.C. § 1681e(b).
[126] CFPB Advisory Opinion on Fair Credit Reporting; Facially False Data, 87 Fed. Reg. 64689 (2022), https://files.consumerfinance.gov/f/documents/cfpb_fair-credit-reporting-facially-false-data_advisory-opinion_2022-10.pdf.
[127] *Id.*
[128] 15 U.S.C. § 1681e(c).
[129] 15 U.S.C. § 1681e(d).
[130] 15 U.S.C. § 1681i.
[131] 15 U.S.C. § 1681i(a)(2)(A).

VI. Thomson Reuters' Apparent Violations of the FTC Act

A. Thomson Reuters' Development and Operation of its Fraud Detect System Constitute Unfair Trade Practices Under the FTC Act

63. Thomson Reuters' development and operation of Fraud Detect—including the acquisition and integration of Pondera Solutions' FraudCaster system,[132] the collection, processing, and intermingling of extensive government and commercial data about consumers,[133] the use of such data to train and operate an automated fraud detection system,[134] and the generation of fraud alerts and risk scores that determine whether someone will continue to receive public benefits and whether state agencies will initiate overpayment proceedings[135]—are unfair because they cause or are likely to cause substantial injury to consumers which is neither reasonably avoidable nor outweighed by countervailing benefits to consumers or competition.[136]

64. Thomson Reuters' development and operation of Fraud Detect have caused or are likely to cause substantial injury to consumers because they subject public benefits claimants to inaccurate and arbitrary fraud analyses, the results of which have deprived and are likely to deprive consumers of public benefits to which they are eligible or subject them to improper benefits overpayment proceedings.

65. On multiple occasions, Thomson Reuters failed to "consider, assess, or take into account the likelihood of false-positive [fraud alerts] or the potential risks false-positive [fraud alerts] posed to consumers."[137] These risks include not only the risk that false-positive fraud alerts could restrict claimants' access to needed public benefits, but also risks of credit harm, reputational harm, emotional distress, and even arrest.[138]

66. Thomson Reuters' apparent failure to adequately test its Fraud Detect system for accuracy and reliability across use cases either before implementing Fraud Detect or at any time while using the system needlessly exposes public benefits claimants to faulty fraud detection procedures. Further, Thomson Reuters developed, marketed, and deployed its Fraud Detect system "without taking reasonable steps to address the risks that [its] deployment of such

[132] Press Release, Thomson Reuters, Thomson Reuters Acquires Pondera Solutions (Mar. 19, 2020), https://perma.cc/7MRG-QPCF.
[133] *See* D.C. Pondera Proposal at 8; Pondera Master Design Document at 5, 7, 10; *Fraud Detect*, Thomson Reuters, https://perma.cc/E585-C459; *see also* Contract between Ill. Dep't of Emp. Sec. & Pondera Solutions 57, https://perma.cc/NQ8M-9QPA; Contract between D.C. Dep't of Hum. Servs. & Pondera Solutions 14–15, https://perma.cc/56C7-WYB3.
[134] *See* D.C. Pondera Proposal at 3, 7; Pondera Master Design Document at 5–6.
[135] *See* Pondera Master Design Document at 4–5; Screened & Scored Report at 25; Lightman, *supra* note 92;
[136] 15 U.S.C. § 45(n); FTC Unfairness Policy Statement.
[137] Rite Aid Order at 11.
[138] *Id.*; *see also* ACLU, *A Pound of Flesh: The Criminalization of Private Debt* 35 (2018), https://www.aclu.org/publications/pound-flesh-criminalization-private-debt.

technology was likely to result in harm to consumers as a result of false-positive [fraud] alerts."[139]

67. Moreover, Thomson Reuters' failure to adequately notify agencies and impacted consumers of how it developed and trained the Fraud Detect system, as well as how the Fraud Detect system generates fraud alerts and risk scores, forces government agencies to blindly rely on Fraud Detect's outputs without the information necessary to evaluate each fraud alert or risk score for accuracy or bias.

68. Consumers cannot reasonably avoid the harm that Thomson Reuters allegedly imposes when it operates Fraud Detect on behalf of state agencies. Thomson Reuters does not publicize or explain its use of Fraud Detect within state public benefits programs,[140] and because Fraud Detect is embedded within many state public benefits programs, consumers must submit to Thomson Reuters' automated fraud detection services to remain within public benefits programs.[141] Further, Thomson Reuters' integration of its CLEAR platform within Fraud Detect extends the potential privacy harms that consumers face when seeking out government assistance; any fraud alerts that Fraud Detect generates in response to a consumer's application or renewal of public benefits will rely not only on the information that consumers consciously provide the government, but also on billions of commercial data points compiled by Thomson Reuters, including data from consumer's social media accounts.[142]

69. The accuracy and bias risks inherent to Fraud Detect are not outweighed by countervailing benefits to consumers or competition. Consumers who are not flagged for fraud by Thomson Reuters' Fraud Detect system receive no benefit that they would not have received in the absence of Fraud Detect, and consumers who are flagged for fraud by the system—more often than not inaccurately[143]—may lose access to their public benefits or may be required to pay state agencies back for alleged overpayments, meaning they are no longer able to benefit from the relevant public benefits program.

70. Further, Thomson Reuters appears to frequently embed its Fraud Detect system within public benefits programs through noncompetitive procurement processes, impeding the competition that would ordinarily be present in competitive bidding processes.[144]

---

[139] *See* Rite Aid Order at 35.

[140] Where consumers have no reason to anticipate harm, as in cases where they lack knowledge of the existence of an unfair practice, "there [i]s no occasion for the consumers even to consider taking steps to avoid it." *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1998).

[141] The "not reasonably avoidable" element of the unfairness doctrine can be satisfied where consumers have no reasonable choice or where consumers are forced to make a certain choice. *See Pa. Funeral Dirs. Ass'n, Inc. v. FTC*, 41 F.3d 81, 91 (3d Cir. 1994); *Am. Fin. Servs. Ass'n v FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985).

[142] *See,* Pondera Master Design Document at 5–6; *cf. also Thomson Reuters CLEAR*, Thomson Reuters, https://perma.cc/7Y7Q-572S.

[143] *See* Cal. Leg. Analyst's Off., *supra* note 4 (finding that Thomson Reuters' Fraud Detect incorrectly flagged 600,000 legitimate claimants as fraudulent, leading to unjust benefits suspension. This finding places Fraud Detect's accuracy rate at 46%.).

[144] *See* Outsourced & Automated Report at 32–35, 87; SHI Int'l Corp., NASPO ValuePoint, SHI Current Product Catalog, https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/shi-international-corp/ (last visited Dec. 18, 2023) (document under Pricing Documents).

B. Thomson Reuters Provides the Means and Instrumentalities for Unfair and Deceptive Acts and Practices When it Contracts with Government Agencies for the Deployment and Maintenance of Fraud Detect in Public Benefits Programs

71. Thomson Reuters furnishes state agencies with the means and instrumentalities for unfair and deceptive acts and practices when it provides the faulty Fraud Detect system to agencies without giving them sufficient information to evaluate the accuracy, reliability, proper use, and use limitations of the Fraud Detect system.

72. Thomson Reuters has marketed Fraud Detect as a "force multiplier" capable of reducing agency costs while increasing insights into public benefits claimants,[145] urging state agencies to rely on the Fraud Detect system when administering and overseeing public benefits programs.

73. Because Thomson Reuters frequently retains control over the operation of Fraud Detect and does not provide training or access to state agency officials to understand and review the Fraud Detect system, state agencies cannot reliably evaluate whether Thomson Reuters' fraud determinations are accurate.[146]

74. Based on faulty fraud determinations made by Thomson Reuters and the Fraud Detect system, state agencies have reduced or revoked public benefits from eligible consumers or demanded money back from eligible consumers.[147]

75. Public benefits determinations based on faulty fraud determinations produced by Thomson Reuters' Fraud Detect are unfair because they cause or are likely to cause substantial injury to consumers which is neither reasonably avoidable nor outweighed by countervailing benefits to consumers or competition.[148]

76. Agencies' faulty reductions or revocations of public benefits to eligible claimants directly and substantially injure claimants financially by withholding or clawing back funds from claimants when they have significant need for financial assistance.

77. Public benefits applicants and claimants have no choice but to defer to an agency's eligibility or fraud determination. Frequently, public benefits claimants receive no explanation when their public benefits are reduced or revoked due to an automated fraud alert or risk

[145] *See* D.C. Pondera Proposal at 7.
[146] *See, e.g.*, Contract between Ill. Dep't Emp. Sec. and Pondera Solutions 45–49, https://epic.org/wp-content/uploads/2023/10/Illinois-FraudCaster-Contract.pdf (Thomson Reuters retaining control over operation of Fraud Detect instead of providing agency with access); Contract between Nevada Dep't Health & Hum. Servs., Div. Welfare & Supportive Servs. and Pondera 13–17, https://epic.org/wp-content/uploads/2023/10/Nevada-Pondera-Contract.pdf (same); Screened & Scored Report at 24 (DC government lacks information on Fraud Detect accuracy testing);
[147] *See* Lightman, *supra* note 92; Cal. Leg. Analyst's Off., *supra* note 4; Screened & Scored Report at 25.
[148] 15 U.S.C. § 45(n); FTC Unfairness Policy Statement.

determination, even though claimants have a Fourteenth Amendment due process right to be provided adequate notice.[149]

78. The alleged injuries imposed by state agencies' procurement and use of Fraud Detect are not outweighed by countervailing benefits to consumers or competition. Consumers who are not flagged for fraud by Thomson Reuters' Fraud Detect system receive no benefit that they would not have received in the absence of Fraud Detect, and consumers who are flagged for fraud by the system—more often than not inaccurately[150]—may lose access to their public benefits or may be required to pay state agencies back for alleged overpayments, meaning they are no longer able to benefit from the relevant public benefits program. Further, any purported benefits of Thomson Reuters' Fraud Detect, such as cost reductions, taxpayer savings, or assistance prioritizing "high-value" fraud cases, are likely outweighed by contract costs imposed by Thomson Reuters itself. For example, EPIC's research into state AI contracts suggests that Thomson Reuters generated up to $30,861,374 in revenue from providing or operating Fraud Detect or similar services in at least 42 states.[151]

VII. Thomson Reuters' Apparent Violations of the Fair Credit Reporting Act

A. Thomson Reuters is a Consumer Reporting Agency under the Fair Credit Reporting Act

79. Through its development, sale, and operation of Fraud Detect, Thomson Reuters regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to state agencies and private healthcare entities and uses the internet and other means or facilities of interstate commerce to do so.

80. Thomson Reuters regularly assembles, evaluates, and furnishes consumer reports via its CLEAR database. Various data points within the CLEAR database used in Thomson Reuters' Fraud Detect fall within the Federal Reserve's Credit Report Definition,[152] including public benefits claimants' names, addresses, social security numbers, dates of birth, employment information, existing debts, and adverse court judgments.[153] Further, a dataset containing consumer report information constitutes a consumer report under FCRA even if

[149] *See, e.g.*, Outsourced & Automated Report at 60; *Mathews v. Eldridge*, 424 U.S. 319, 325–26 (1976); *Goldberg v. Kelly*, 397 U.S. 254, 266–71 (1970); *Elder v. Gillespie*, 54 F.4th 1055, 1065 (8th Cir. 2022); Screened & Scored Report at 33; Mallory Sofastaii, *Even with New System, Unemployment Calls Continue to Overwhelm Phone Lines*, WMAR Baltimore (June 10, 2020), https://perma.cc/RZ7W-9U2K.
[150] *See* Cal. Leg. Analyst's Off., *supra* note 4 (finding that Thomson Reuters' Fraud Detect incorrectly flagged 600,000 legitimate claimants as fraudulent, leading to unjust benefits suspension. This finding places Fraud Detect's accuracy rate at 46%.).
[151] Outsourced & Automated Report at 39.
[152] Bd. Governors Fed. Rsrv. Sys., Consumer's Guide: Credit Reports and Credit Scores, https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf (last visited Dec. 18, 2023).
[153] Pondera Master Design Document at 5; *see also* Contract Between Il. Dep't Emp. Sec. and Pondera Solutions 21, https://perma.cc/NQ8M-9QPA.

the dataset includes other information and was not expected to be used for a FCRA-related purpose.[154]

81. Thomson Reuters' reliance on Fraud Detect to automatically generate fraud alerts and risk scores based on consumer credit information does not relieve Thomson Reuters of its FCRA obligations. A company's collection and use of consumer data within an automated scoring system is covered by FCRA even when the company does not directly analyze the data that informed the score.[155]

82. For the foregoing reasons, Thomson Reuters is a CRA under FCRA and must abide by all relevant FCRA requirements, including those laid out in Sections 605, 607(b)–(d), and 6011 of FCRA.

B. Thomson Reuters Has Failed to Meet its Statutory Obligations as a Consumer Reporting Agency Under the Fair Credit Reporting Act

83. Thomson Reuters appears to have violated Section 605 of FCRA by including prohibited items of information within the consumer reports it furnishes to agencies and private healthcare entities. Thomson Reuters does not appear to remove old civil and criminal judgments or other adverse actions from its CLEAR database, even when those data antedate a furnished consumer report by more than seven to ten years.[156]

84. Thomson Reuters appears to have violated Section 607(b) of FCRA by failing to maintain reasonable procedures to assure maximum accuracy of the information it furnishes to agencies and private healthcare entities through its Fraud Detect system. Thomson Reuters has not demonstrated that it adequately tests or evaluates the accuracy of its Fraud Detect system. Rather, the Fraud Detect system appears to furnish inaccurate consumer information to state agencies more often than not.[157] And although some state contracts require Thomson Reuters to conduct data privacy and security assessments,[158] those assessments do not measure the *accuracy* of information within Thomson Reuters CLEAR database or Fraud Detect system.

85. Thomson Reuters appears to have violated Section 607(c) of FCRA by withholding key consumer report information from state agencies, thereby preventing the agencies from disclosing the contents of fraud alerts and risk scores generated by Fraud Detect to impacted consumers following adverse actions. Because Thomson Reuters often maintains sole operational control over the Fraud Detect system and withholds key information about the

[154] *See* Chi Chi Wu et al., Nat'l Consumer L. Ctr., Fair Credit Reporting § 2.3.5.4 45–47 (10th ed. 2022) (citing FTC, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations § 603(d)(1) Items 4, 5c, & 7d (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf). 445 (10th ed. 2022); *id.* at § 2.3.5.2 43 (citing 15 U.S.C. § 1681a(d)).
[155] *See Heagerty v. Equifax Info. Servs. LLC*, 447 F.Supp.3d 1328, 1345 (N.D. Ga. 2020).
[156] *See* 15 U.S.C. § 1681c(a).
[157] *See* Cal. Leg. Analyst's Off., *supra* note 4.
[158] *See, e.g.*, Contract between Ind. Fam. & Soc. Servs. Admin. and West Publishing 11, https://epic.org/wp-content/uploads/2023/10/Indiana-FSSA-FraudCaster-Contract.pdf.

Fraud Detect system (on the grounds that doing so stymies fraudsters),[159] agencies that rely on consumer report information furnished through the Fraud Detect system rarely know why Fraud Detect generates certain consumer fraud determinations.

86. Thomson Reuters appears to have violated Section 607(d) of FCRA by failing to notify state agencies and private healthcare companies that rely on Fraud Detect about their obligations under FCRA. Instead of furnishing such notice, Thomson Reuters attempts to disclaim that it is a CRA under FCRA and require that the "data provided to [Fraud Detect customers] may not be used as a factor in… establishing a consumer's eligibility for… government benefits."[160] On the same webpage, however, Thomson Reuters specifically markets its Fraud Detect system as a tool for public benefits programs like unemployment insurance and the Supplemental Nutrition Assistance Program (SNAP).[161]

87. Thomson Reuters appears to have violated Section 611 of FCRA by failing to reinvestigate the accuracy of consumer information within its CLEAR database or Fraud Detect system following consumer disputes. EPIC found no correction, consumer dispute, or reinvestigation provision within any of the Fraud Detect contracts it identified across the country.[162]

VIII. Prayer for Investigation and Relief

70. EPIC urges the Commission to investigate Thomson Reuters to determine if Thomson Reuters, by developing, selling, and operating its Fraud Detect product, has engaged in unfair and deceptive trade practices under Section 5 of the FTC Act and violated the Fair Credit Reporting Act. At a minimum, the FTC should investigate to what extent Thomson Reuters and its subsidiaries engage in the following practices:

    a. Collecting, retaining, and using consumer data without investigating—or, after a consumer dispute, reinvestigating—the data's accuracy, completeness, or reliability as an indicator of fraud;

[159] Thomson Reuters, *Follow the Money: Fighting Fraud in the Unemployment Insurance System During COVID-19*, https://perma.cc/BYR6-M7XA; *see also* Jon Coss, *Catching Bad Guys: Preventing and Combating Fraud in Government Programs*, Thomson Reuters, https://perma.cc/Y3W9-ZB5J.
[160] *See Improve Fraud Detection and Prevention with Fraud Detect*, Thomson Reuters, https://perma.cc/CH47-VTEX.
[161] *Id.*
[162] *See generally* DC Pondera Proposal; Pondera Master Design Document; Contract Between Il. Dep't Emp. Sec. and Pondera Solutions, https://perma.cc/NQ8M-9QPA; Contract between Iowa Dep't Pub. Health & Pondera Solutions, https://epic.org/wp-content/uploads/2023/10/FY19_Iowa_Service_Contract_Pondera_Solutions.pdf; Contract between Nev. Dep't Health & Hum. Servs. & Pondera Solutions, https://epic.org/wp-content/uploads/2023/10/PonderaContract-FullyExecuted-1.pdf; Contract between Ind. Dep't Workforce Dev. and Pondera Solutions, https://epic.org/wp-content/uploads/2023/10/Indiana-FraudCaster-Contract.pdf; Contract between Ind. Fam. & Soc. Servs. Admin. and West Publishing, https://epic.org/wp-content/uploads/2023/10/Indiana-FSSA-FraudCaster-Contract.pdf. For more information on these contracts, see generally Outsourced & Automated Report.

b. Collecting, retaining, and using data about civil and criminal judgments or other adverse actions that antedate furnished consumer reports by the statutory periods listed in Section 605 of FCRA;[163]

b. Selling the Fraud Detect system to public agencies or operating Fraud Detect on behalf of public agencies without disclosing Fraud Detect's accuracy rates and use limitations;

c. Developing, marketing, or operating Fraud Detect without testing, auditing, or otherwise evaluating the Fraud Detect system for accuracy and bias;

d. Failing to notify public agencies of their obligations under FCRA, given Thomson Reuters' status as a CRA; or

e. Failing to reinvestigate the accuracy of consumer information within Thomson Reuters' CLEAR database or Fraud Detect system following a consumer dispute under Section 611 of FCRA.[164]

71. EPIC further urges the Commission to:

a. Direct Thomson Reuters to comply with FCRA to the extent it acts as a consumer reporting agency under the Act;

b. Require Thomson Reuters to comply with existing public policy frameworks for responsible AI development and use, including the OECD AI Principles, the Universal Guidelines for AI, and Executive Order 14110;

c. Halt any unlawful or impermissible retention, use, and disclosure of consumer report information furnished by Thomson Reuters through the Fraud Detect system, including, but not limited to, civil judgments, accounts placed for collection, and other adverse actions outside the permissible time period established by Section 605 of FCRA;[165]

d. Require that Thomson Reuters and its subsidiaries notify any public benefits claimants whose data Thomson Reuters has improperly disclosed in violation of FCRA or whose access to or eligibility for public benefits was negatively impacted by an incorrect alert, risk score, or determination generated by the Fraud Detect system;

e. Require Thomson Reuters to provide a written notice explaining the precise basis for any fraud determinations or recommendations for further investigation, public benefits revocation, or denial of a public benefits application to any customers and claimants subject to an adverse action because of the Fraud Detect system;

[163] 15 U.S.C. § 1681c.
[164] 15 U.S.C. § 1681i.
[165] 15 U.S.C. § 1681c.

f. Require Thomson Reuters and its subsidiaries to implement and maintain an effective AI testing, evaluation, and monitoring program to detect and mitigate errors or biases within the Fraud Detect system both before and during deployment;[166]

g. Require Thomson Reuters to delete or destroy any data, models, or algorithms related to the Fraud Detect system that are either derived from illegally collected, retained, or used consumer data or deployed in ways that impose an impermissible risk of errors, biases, or other consumer harms;[167]

h. Prohibit Thomson Reuters from misrepresenting in any manner, expressly or by implication, the accuracy of the Fraud Detect system or the extent to which it uses commercial consumer data to calculate public benefits fraud alerts and risk scores;[168]

i. Require Thomson Reuters to obtain initial and ongoing AI audits of the Fraud Detect system from a "qualified, objective, independent third-party professional" who "uses procedures and standards generally accepted in the profession;"[169]

j. Require Thomson Reuters to provide such other information or documentation which may be necessary to ensure compliance with the aforementioned monitoring and notice requirements, including but not limited to compliance reports, model cards, and incident reports;[170] and

k. Provide such other relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

/s/ John Davisson
John Davisson
Director of Litigation
davisson@epic.org

/s/ Ben Winters
Ben Winters
Senior Counsel
winters@epic.org

/s/ Grant Fergusson
Grant Fergusson
Equal Justice Works Fellow

[166] This monitoring program could mirror similar AI monitoring programs mandated by FTC orders. *See, e.g.*, Rite Aid Order at 7–13.
[167] *See id.* at 6–7.
[168] *See id.* at 16–17.
[169] *See id.* at 21–23.
[170] *See id.* at 24–26.

fergusson@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)