

EPIC Screening and Scoring Spotlight: Pondera's Fraud Prediction Algorithms for Public Benefits

Government agencies across the country are using third-party algorithms in attempts to predict, prevent, and investigate fraud in public benefits programs.

As part of EPIC's Screening and Scoring Project, we are taking an in-depth look into Pondera Solutions, one company among many touting their ability to digitally predict and prevent public benefits fraud. EPIC submitted over a dozen public records requests to public agencies in California, the District of Columbia, Georgia, Illinois, Indiana, Iowa, Kansas, Louisiana, Massachusetts, Montana, Nevada, and South Carolina. We have received responsive documents from some states and are awaiting responses from others. In addition, EPIC undertook significant documentary and legislative research to learn more about how Pondera's software works and its relationship with different state agencies.

EPIC's research into Pondera is ongoing. This page will be periodically updated with relevant analysis and documents produced from open records requests.

Pondera's Predictive Tools

Pondera, acquired by Thomson Reuters in 2020, sells technologies that promise to prevent fraud in healthcare and programs such as unemployment insurance, Pandemic Unemployment Insurance, and the supplemental nutrition assistance program (SNAP). The scope of Pondera's business with state and federal government agencies is unclear, but in 2018, before a period of very aggressive growth, Pondera was working with 30 agencies in eight states.

Pondera touts that they can "minimize risk and reduce fraud" with two of their products: CaseTracker, an investigation management system, and Fraudcaster, a tool for predicting fraud. When jurisdictions contract with Pondera, they often license both.

Fraudcaster numerically scores public benefits applicants and recipients based on their purported likelihood of committing fraud, drawing on data from data brokers, social media scrapers, credit reporting agencies, location servicers, and government records databases. The company claims this fraud risk score is meant to prioritize enforcement resources for agencies.

The type of information collected includes applicants' race, disability, citizenship, criminal history, failure to report income, homelessness status, income, household composition, "overpayments," Medicaid assistance, paternity, and "purpose of care," and more.

The system then analyzes the data to produce tiers of alerts or flags for investigators.

For example, alerts or flags for possible SNAP benefits fraud include:

- Deceased or incarcerated recipient
- Prolonged or exclusive out-of-state EBT use
- ID theft
- Recipients traveling 25 miles or more for their shopping
- “Excessive” address changes
- Two or more households using the same IP address

The FDaaS-NV-DWSS system may interface with the following systems:

1. Dun & Bradstreet (Public Records)

2. Appriss Corporation (Public Records and Criminal History)
3. TLOxp Corporation (Public Records)
4. Wist / Hamari (link analysis implementation co-located with FDaaS instance)
5. Google Corporation (Maps, Fusion Tables, and Prediction APIs)
6. LexisNexis (public records, licensure records)
7. Social Intelligence (social media lookups)

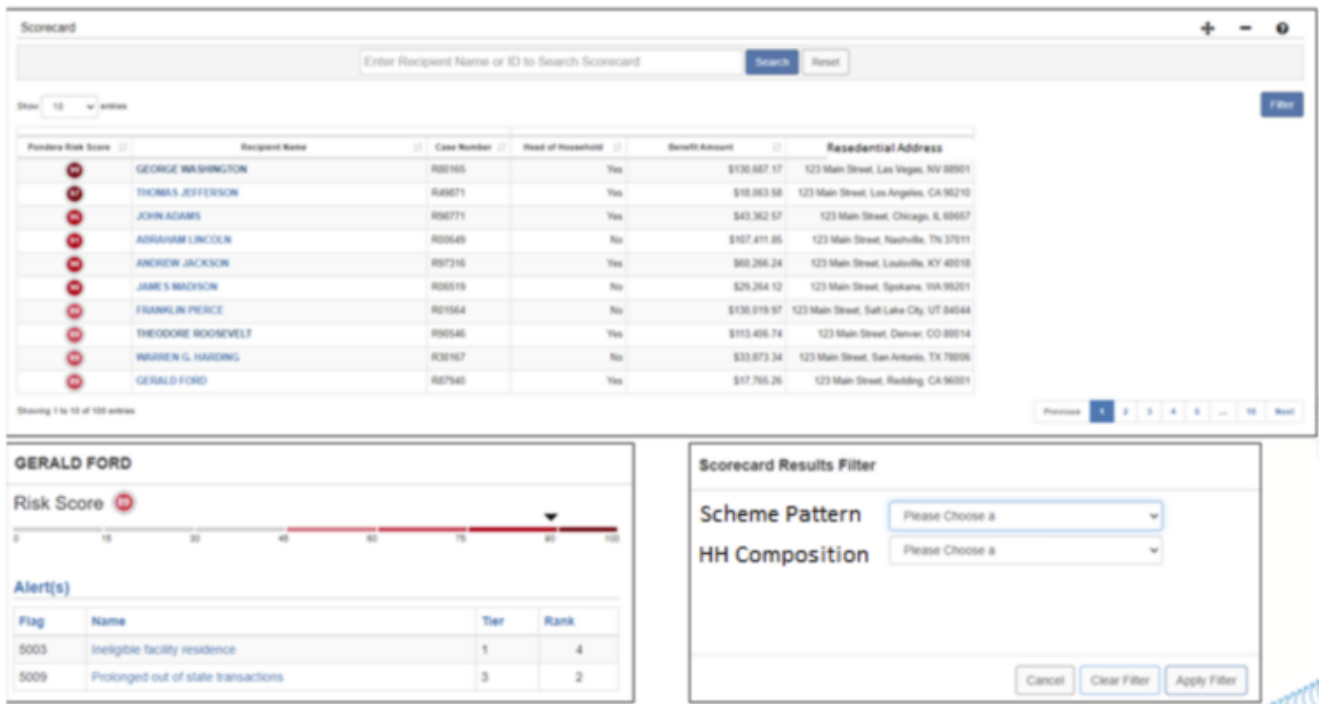
A list of systems that Fraudcaster may interact with, NV DHHS FDaaS System Security Plan

Figure 3: Alert Categorization Key

Tier Types	
1	Potential for Fraud/Risk
2	Highly Suspect
3	Needs Review
4	Suspect Element
5	Informational Data Point

An Alert Categorization Key will factor in additional data like Alert Tier Types, DC DHS Master Design Document

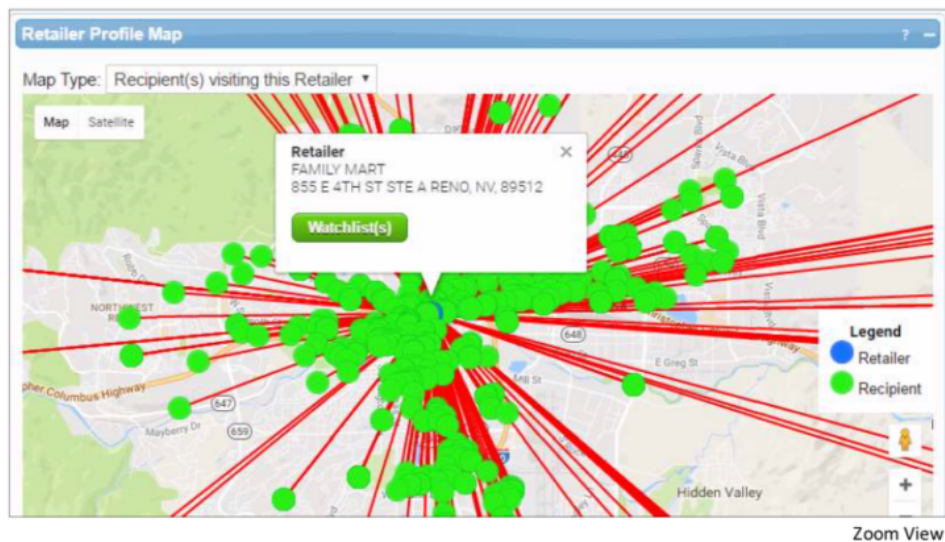
FraudCaster continually updates its scorecard to prioritize families, individuals, and entities for agency investigation. Outcome data from CaseTracker is used to “fine tune” Pondera’s risk scoring algorithm to prioritize highest risk cases to the top.



Examples of scorecard results, DC DHS Master Design Document

FraudCaster displays results via a dashboard that includes alerts, geospatial mapping, entity profiles, validity scores, and "investigation recommendations." Pondera does not make public any of its error rates.

Family Mart Geospatial Map – Recipients Visiting Retailer



Geospatial mapping for purported SNAP trafficking by a retailer, NV Legislative Intel Brief

Our Concerns

Pondera's software makes decisions that dramatically impact people's lives, potentially cutting them off from the emergency benefits they need to remain in their homes and feed their families. But details about how—or even whether—Pondera's software works correctly are extremely difficult to find.

The documents EPIC received have bolstered several concerns about how these tools are used, including:

- There is a lack of transparency about logic underlying FraudCaster's risk predictions;
- Pondera, like other private companies, shields their algorithms from public scrutiny, making it difficult to know how they generate a risk score;
- Pondera's risk model is built on information gathered about "households" and networks—not just individuals—and those who are targeted and investigated are rarely aware of it;
- Pondera relies on an enormous volume of sensitive, personal data to be useful. The company's reach and data sharing further feeds into a surveillance state;
- Contracts have insufficient data protection for the responsible use of surveillance-based tools (such as use restrictions, data minimization requirements, purpose specifications, and data proportionality measures);
- Pondera promises to *predict* and *prevent* fraud, but the tools can just as easily be used to look backwards through agency data, identifying purported "overpayments" for the purpose of aggressive debt collection.

Beyond the technology, Pondera's business practices and profit motives exemplify how technology companies are entrenching themselves in government administration. Jon Coss, Pondera CEO, has publicly stated that in some states, he believes that 75% of applications to federal programs are "very likely fraud." Pondera's software is expensive and it is unclear whether there is actually a significant return on investment for states—or if "return on investment" is a meaningful metric by which to judge the integrity of programs that provide life-saving resources to millions of Americans.

PONDERA'S CONNECTION WITH THOMSON REUTERS

Thomson Reuters collects "billions of data points" about individuals, combines the data points into searchable dossiers, and sells these dossiers through its CLEAR platform. In several contracts, Pondera gives free trials to CLEAR, Thomson Reuters' controversial data broker operations, and License Plate Recognition (LPR). Free trials of CLEAR and LPR further stray from the contract's purpose specification of fraud investigation.

Thomson Reuters has fallen under scrutiny for illegally selling personal data without people's consent to law enforcement agencies, including U.S. Immigration and Customs Enforcement. A coalition of activists sued Thompson Reuters, accusing the company of illegally selling data of California residents without their consent.

It is not clear whether citizen data provided to Pondera is also obtained, used, and sold by Thomson Reuters.

Key Documents

So far, EPIC has received requests for proposals, executed contracts, master design documents, legislative intelligence briefs, implementation summaries, data sharing agreements, and data dictionaries (which list variables included in the predictive software service and define them). Below are key documents that have helped us understand how states have contracted with Pondera and how Pondera's predictive technology works.

- [Pondera FraudCaster Master Design Document](#) (D.C. Department of Human Services)
- [Pondera Fraudcaster Master Design Document](#) (Nevada Department of Health and Human Services)
- [California Data Use Agreement Example for Nevada](#) (Nevada Department of Health and Human Services)
- [Fraud Profile Indicators](#) (Nevada Department of Health and Human Services)
- [FDaaS Implementation Summary FINAL](#) (Nevada Department of Health and Human Services)
- [FDaaS Implementation Summary REDACTED](#) (Nevada Department of Health and Human Services)
- [FDaaS System Security Plan](#) (Nevada Department of Health and Human Services)
- [Glossary of Terms](#) (Nevada Department of Health and Human Services)
- [Glossary of Terms March 2016](#) (Nevada Department of Health and Human Services)
- [Pondera Legislative Intel Brief](#) (Nevada Department of Health and Human Services)

STATE CONTRACTS

- [Pondera-Illinois Contract](#) (Illinois Department of Employment Security)
- [Pondera-DC Contract](#) (D.C. Department of Human Services)



1519 New Hampshire Avenue NW

Washington, DC 20036

202.483.1140 | info@epic.org

Sign Up for EPIC Alerts

Email address

SUBSCRIBE

EPIC uses EmailOctopus to maintain our mailing list and send newsletters. [View EmailOctopus' privacy policy.](#)

ISSUES

- AI & Human Rights
- Consumer Privacy
- Cybersecurity
- Data Protection
- Democracy & Free Speech
- Open Government
- Platform Accountability & Governance
- Privacy Laws
- Surveillance Oversight

OUR WORK

- Updates
- Analysis
- EPIC Alert
- Events
- EPIC Publications
- Digital Library

MEDIA

- EPIC in the News
- Press Kit
- EPIC Statements
- EPIC Commentaries

ABOUT

- EPIC Projects
- Board & Staff
- EPIC Advisory Board
- Careers & Internships
- Being a Non-profit
- Cy Pres Awards
- Privacy Policy
- Contact Us

DONATE →