[Cite as *The Markup v. Ohio Dept. of Job & Family Servs.*, 2023-Ohio-623.]

IN THE COURT OF CLAIMS OF OHIO

THE MARKUP Requester v. OHIO DEPARTMENT OF JOB AND FAMILY SERVICES Respondent	Case No. 2022-00279PQ Special Master Jeff Clark REPORT AND RECOMMENDATION

{¶1} This case arises from a public records request made by a journalist intending to publish articles about the nature of a computerized fraud prediction system implemented by the Ohio agency that processes unemployment insurance benefits. Unless proven exempt by law from disclosure, Ohio's Public Records Act requires officials to make copies of public records available "upon request by any person." R.C. 149.43(A)(1), (B)(1). The Act must be construed liberally in favor of broad access, and any doubt is resolved in favor of disclosure of public records. *State ex rel. Rogers v. Dept. of Rehab. & Corr*., 155 Ohio St.3d 545, 2018-Ohio-5111, 122 N.E.3d 1208, ¶ 6. R.C. 2743.75 provides a special statutory proceeding to enforce the Act in this court.

{¶2} "One of the salutary purposes of the Public Records Law is to ensure accountability of government to those being governed." *Strothers v. Wertheim*, 80 Ohio St.3d 155, 158, 684 N.E.2d 1239 (1997). Journalists utilize the Act for this purpose:

> "(I)n a society in which each individual has but limited time and resources with which to observe at first hand the operations of his government, he relies necessarily upon the press to bring to him in convenient form the facts of those operations. Great responsibility is accordingly placed upon the news media to report fully and accurately the proceedings of government, and official records and documents open to the public are the basic data of governmental operations."

Kallstrom v. City of Columbus, 165 F.Supp.2d 686, 697 (S.D.Ohio 2001), quoting *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 492, 95 S.Ct. 1029, 43 L.Ed.2d 328 (1975). The Ohio Supreme Court is in wholehearted agreement "as to the importance of the media in gathering and disseminating information to the public," *State ex rel. Cincinnati Enquirer v. Pike Cty. Coroner's Office*, 153 Ohio St.3d 63, 2017-Ohio-8988, 101 N.E.3d 396, ¶ 54, because

> [p]ublic records are one portal through which the people observe their government, ensuring its accountability, integrity, and equity while minimizing sovereign mischief and malfeasance. *See, e.g. State ex rel. Gannett Satellite Information Network, Inc. v. Petro* (1997), 80 Ohio St.3d 261, 264, 1997 Ohio 319, 685 N.E.2d 1223; *State ex rel. Strothers v. Wertheim* (1997), 80 Ohio St.3d 155, 157, 1997 Ohio 349, 684 N.E.2d 1239. Public records afford an array of other utilitarian purposes necessary to a sophisticated democracy: they illuminate and foster understanding of the rationale underlying state decisions, *White* [*v. Clinton Cty. Bd. of Commrs*., 76 Ohio St.3d 416, 420, 667 N.E.2d 1223 (1996)], promote cherished rights such as freedom of speech and press, *State ex rel. Dayton Newspapers, Inc. v. Phillips* (1976), 46 Ohio St.2d 457, 467, 75 O.O.2d 511, 351 N.E.2d 127, and "foster openness and * * * encourage the free flow of information where it is not prohibited by law." *State ex rel. The Miami Student v. Miami Univ*. (1997), 79 Ohio St.3d 168, 172, 1997 Ohio 386, 680 N.E.2d 956.
>
> (Ellipsis sic.) *Kish v. Akron*, 109 Ohio St.3d 162, 2006-Ohio-1244, 846 N.E.2d 811, ¶ 16.

Id. at ¶ 53.

{¶3} On November 29, 2021, requester Todd Feathers, a journalist for a New York-based[1] media organization called The Markup,[2] made a public records request to respondent Ohio Department of Job and Family Services (ODJFS) for:

1) All weekly status reports submitted to the department by Google and/or Carasoft and their subsidiaries with regards to the attached contract (page four of the pdf, under the "Data Load & Analytics" section.

2) All "reports on discovered patterns and behaviors identified in the analysis of the data provided" submitted to the department by Google and/or

[1] "Any person" includes foreign-state residents. 2006 Ohio Atty.Gen.Ops. No. 2006-038.

[2] Although Feathers entered "The Markup" in the field for "Name of person **or** organization that made public records request" on the complaint form, the November 29, 2021 request and all follow-up correspondence was made solely in Feathers' name. The Special Master determined that Feathers is the real party in interest and that despite misnaming his media organization as the "requester" this action is brought by an individual person rather than a corporation. (July 27, 2022 Order.)

Carahasoft and their subsidiaries with regards to the attached contract (page four of the pdf, under the "Data Load & Analytics" section).

3) All "modeling and design validation guidelines" submitted to the department by Google and/or Carahasoft and their subsidiaries with regards to the attached contract (page four of the pdf, under the "Data Load & Analytics" section).

4) All documents containing "analysis of the data to determine the likely indicator or combination of indicators that might otherwise indicate that a given record is or is not eligible" submitted to the department by Google and/or Carahasoft and their subsidiaries with regards to the attached contract (page four of the pdf, under the "Data Load & Analytics" section).

5) All "detailed documentation on exploratory analysis and analytics and knowledge transfer" submitted to the department by Google and/or Carahasoft and their subsidiaries with regards to the attached contract (page five of the pdf, under the "Deliverables" section).

(Complaint at 5.) On March 23, 2022, ODJFS produced records in response to Request No. 1 with redactions based on the security and infrastructure exemptions in R.C. 149.433. (*Id*. at 7.) ODJFS initially stated it was unable to fulfill Requests Nos. 2-5 because they sought information rather than records and did not "identify, with reasonable clarity, the records you seek." (*Id*.) However, ODJFS no longer asserts that Requests #2 through #5 are overly broad. (Response at 6.)

{¶4} On March 28, 2022, Feathers filed a complaint pursuant to R.C. 2743.75 alleging denial of access to public records in violation of R.C. 149.43(B). Following mediation, ODJFS filed a response and motion to dismiss (Response) on June 8, 2022. On June 28, 2022, Feathers filed a reply. On October 27, 2022, ODJFS filed a sur-reply, and also filed withheld records under seal. On January 11, 2023, ODJFS filed additional withheld records under seal, and an explanatory pleading.

Unemployment Insurance Fraud Prediction System

{¶5} In response to fraud occurring in its distribution of state and federal moneys, ODJFS contracted with Google and Carahsoft to supply a computer application – the "Google Fraud Dashboard" – that can predict the likelihood of fraud in unemployment insurance claims submitted to the department. (Response at 2-4, Exh. 2 – Sines Aff. at ¶ 8, Exh. 3 – Prideau Aff. at ¶ 15.) The Dashboard applies algorithms to data factors

selected by ODJFS to create a model against which unemployment insurance applications are compared. (*Id*. at ¶ 9.) If an application contains data factors that rise to a weight or threshold level set by ODJFS, it is flagged as potentially fraudulent and reviewed by an ODJFS employee. (Sines Aff. at ¶ 10.) The factors, weights and thresholds are continually adjusted in response to observed fraud patterns. (*Id*. at ¶ 9.)

{¶6} Software used to operate a computer is usually just the means of access to records, without itself meeting the definition of a "record." *State ex rel. Recodat Co. v. Buchanan*, 46 Ohio St.3d 163, 165, 546 N.E.2d 203 (1989). Application software is not a "record" subject to the Public Records Act unless, and then only to the extent that, it documents the activities of the office. In this case, the Dashboard is not a shrink-wrapped commercial software product but a custom application programmed in part with institutional data factors, weights, and threshold values. These parts of the Dashboard programming serve to document policy decisions made by ODJFS in the evolving configuration of its fraud control procedures. Documents kept by ODJFS that reflect these choices thus meet the definition of "records" of the office, R.C. 149.011(G).

Responsive Records Provided, With Redactions

{¶7} Feathers confirms that the documents referenced in Request #1 have been provided. (Reply at 1.) During litigation, ODJFS produced additional emails responsive to Request #1 as well as a Technical Design Document (TDD) responsive to Requests #2 through #5. (Response at 6, Exh. 1 – Sullivan Aff. at ¶ 4-5, Exh. 2 – Sines Aff. at ¶ 15.b.; Reply at 1, 129-188 – redacted copy of TDD) Feathers has not asserted that any additional records exist responsive to his requests.

{¶8} ODJFS does not dispute that these records are, absent applicable exemptions, public records kept by a public office. The issue before the court is whether ODJFS properly applied public records exemptions to redact information within the documents provided. To its credit, and facilitating the court's review, ODJFS' redactions largely avoid obscuring email and TDD text other than the particular information described in its pleadings and affidavits as subject to the claimed exemptions, in compliance with R.C. 149.43(B)(1).[3]

[3] Based on comparison with the unredacted documents *in camera*. R.C. 149.43(B)(1) provides in pertinent part: "If a public record contains information that is exempt from the duty to permit public inspection

Burden to Prove Exemptions[4]

{¶9} The burden to establish the applicability of an exemption rests on the public office. *Cincinnati Enquirer v. Pike Cty. Coroner's Office*, 153 Ohio St.3d 63, 2017-Ohio-8988, 101 N.E.3d 396, ¶ 15. Exceptions to disclosure are strictly construed against the public-records custodian. *Rogers v. Dept. of Rehab. & Corr*., 155 Ohio St.3d 545, 2018-Ohio-5111, 122 N.E.3d 1208, ¶ 7. A custodian does not meet this burden if it has not proven that the requested records fall squarely within the exception. *State ex rel. Cincinnati Enquirer v. Jones-Kelley*, 118 Ohio St.3d 81, 2008-Ohio-1770, 886 N.E.2d 206, paragraph two of the syllabus. When a public office claims exceptions based on risks that are not evident within the records themselves, the office must provide more than conclusory statements in affidavits to prove the assertion. *State ex rel. Besser v. Ohio State Univ*., 89 Ohio St.3d 396, 400-404, 732 N.E.2d 373 (2000). Any doubt should be resolved in favor of disclosure of public records. *State ex rel. James v. Ohio State Univ.*, 70 Ohio St.3d 168, 169, 637 N.E.2d 911 (1994).

{¶10} ODJFS first asserts that portions of the records were redacted pursuant to R.C. 149.433 as "infrastructure records," "security records," or both. (Response at 9-14; Supp. Response, Exh. 5 – Privilege Log *passim*.) These exemptions are separately defined and will be analyzed separately.

Infrastructure Records

{¶11} R.C. 149.433(A) provides that:

> "Infrastructure record" means any record that discloses the configuration of critical systems including, but not limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of a building.

By this language, listed systems are potentially but not automatically "critical" systems. "Critical," in the context of systems, means "extremely important to the progress or

---

or to copy the public record, the public office * * * shall make available all of the information within the public record that is not exempt." See also R.C. 149.43(A)(13) "Redaction" means obscuring or deleting any information that is exempt from the duty to permit public inspection or copying from an item that otherwise meets the definition of a "record" in section 149.011 of the Revised Code.

[4] A public records exception is a law prohibiting or excusing disclosure of records that would otherwise be public. The terms "exemption" and "exception" are used interchangeably in this report.

success of something." See https://dictionary.cambridge.org/us/dictionary/english/critical (Accessed Nov. 17, 2022.)

{¶12} ODJFS provides the testimony of information security and fraud control staff that the computerized Google Fraud Dashboard is an important component of efforts to prevent, detect, and mitigate incidents of fraud occurring in the state's Unemployment Insurance Program. (Response at 4, Exh. 2 – Sines Aff. at ¶ 8 and 15d., Exh. 3 – Prideau Aff. at ¶ 15; Sur-reply at 2-6.) ODJFS states that hundreds of millions of dollars in unemployment insurance payments have been and continue to be obtained from ODJFS fraudulently (Response, Exh. 3 – Prideau Aff. at ¶ 10-14) and argues that these massive losses would be even worse but for use of the Dashboard.

{¶13} Feathers argues that the system is not a "critical" one because the contract to develop the Dashboard provides that the program need only operate at a "moderate level baseline" as defined in National Institute of Standards and Technology 800-53 Rev. 3. (Reply at 2, Exh. 1 at 38.) ODJFS counters that the "critical" nature of a system is not determined by design criteria or industry standards but by the impact on the office of loss of confidentiality, integrity, or availability of the system. (Sur-reply at 3-5.) ODJFS attests that release of Dashboard information could be expected to have a serious adverse effect on organizational operations, including a significant degradation in mission capability to an extent and duration that the organization may still be able to perform its primary functions, but the effectiveness of those functions is significantly reduced. (Sur-reply, Exh. 4 - Supp. Sines Aff. at ¶ 5-13.) Feathers further emphasizes that ODJFS has lost hundreds of millions of dollars to fraud *despite* the use of the Dashboard. However, past and continuing loss of funds does not make the program's design and purpose any less "critical." Weighing the evidence submitted, the Special Master concludes that ODJFS has shown that the Dashboard falls squarely within the meaning of the term "critical system" as used in R.C. 149.433(A).

{¶14} ODJFS next attests that portions of the requested documents meet the statutory definition by disclosing the "configuration of" this critical system. In common usage, the configuration of a system is the arrangement or relationship of its elements. See merriam-webster.com/dictionary/configuration (Accessed Feb. 7, 2023.) Examples of records that disclose system configuration include electrical schematics, HVAC plans,

computer network diagrams, plumbing layouts, and security code generation algorithms. *Shaffer v. Budish*, Ct. of Cl. No. 2017-00690-PQ, 2018-Ohio-1539, ¶ 18.

{¶15} ODJFS asserts that the factors used in the Dashboard software to flag potentially fraudulent applications, and the weights and thresholds assigned to each factor that then trigger detailed review, "constitute 'relative arrangements of parts or elements,' or the 'configuration' of a critical system—software used to detect fraud in applications." (Response at 11.) ODJFS submits the affidavit of its former Agency Chief Information Security Officer, now Deputy Director of IT Risk and Compliance, who attests that:

1. Redactions to the weekly status reports of SpringML/Google removed specific references to how the models were created and information and data that was used to create them. (Response, Exh. 2 - Sines Aff. at ¶ 15a.)
2. Redactions of the Technical Design Document would disclose how the Google Fraud Dashboard AI/ML models were architected, and obscure diagrams and text containing specifics to the Ohio Job Insurance Database tables and fields, file names, job names, and to the weight, factors, and conditions used to create the models for the Dashboard. (*Id.* at ¶ 15b.), and
3. Redactions of the May 13, 2021 email and attachment from John Skinner to Ward Loving contain data, flags, and insights into the model for the Dashboard. (*Id.* at ¶ 15c.)

{¶16} The Special Master finds that the data factors, flags, weights, and thresholds entered into the Dashboard software meet the definition of "infrastructure records." Review of the redacted information *in camera* shows that for the most part ODJFS has redacted material that falls squarely within the exemption as listed in the privilege log. However, ODJFS was overinclusive in redacting some chapter titles, two sentences that merely contain the word "configuration," and certain other innocuous text.

{¶17} In isolation, merely showing the name or picture of a system component without juxtaposing it with other components does not reveal the *configuration* of the system. *Shaffer v. Budish*, Ct. of Cl. No. 2017-00690-PQ, 2018-Ohio-1539, ¶ 16-18. Moreover, the general principles and indicators of computerized fraud detection systems are not secret. The court may take notice that some features of the Google Fraud

Dashboard in general and Carahsoft modifications in particular have been disclosed in legal and promotional materials available to the public. The general principles and parameters of the system are available online by a web search of “google fraud detection states.” See also Google’s patent for fraud detection using predictive modeling at https://patents.google.com/patent/US5819226A/en. (Accessed Feb. 3, 2023). Carahsoft has posted blogs and public webinars explaining that fraud indicators specifically include repetitive appearance of phone numbers, email addresses and other contact information in multiple claims. See, e.g., https://www.carahsoft.com/blog/f5-unemployment-fraud-impact-blog-2021. (Accessed Feb. 3, 2023.) These application and payment data indicators are similar to other economic crime and fraud indicators that law enforcement agencies generally do not keep secret, but instead publicize to help the public detect and report offenses. However, it is the role of the legislature and not the courts to determine public policy and define the particular records it subjects to a statutory exemption. *State ex rel. WBNS TV, Inc. v. Dues*, 101 Ohio St.3d 406, 2004-Ohio-1497, 805 N.E.2d 1116, ¶ 36-37.

{¶18} The combination of factors, flags, weights, and thresholds developed for ODJFS is unique to the agency’s particular implementation of the fraud-detecting Dashboard. The Special Master concludes that most of the information so identified in ODJFS’ privilege log falls squarely under the statutory definition of “infrastructure record,” with the few exceptions identified in the tables at the end of this report.

Security Records

{¶19} R.C. 149.433 provides, in pertinent part:

> (A) As used in this section: * * * “Security record” means any of the following:
>
> > (1) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage; * * *
>
> (B)(1) A record kept by a public office that is a security record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

{¶20} To meet the burden of proof regarding alleged security records, a public office must offer more than its own conclusory labeling:

> The department and other agencies of state government cannot simply label a criminal or safety record a "security record" and preclude it from release under the public-records law, without showing that it falls within the definition in R.C. 149.433.

State ex rel. Plunderbund Media, L.L.C. v. Born, 141 Ohio St.3d 422, 2014-Ohio-3679, 25 N.E.3d 988, ¶ 29. Even records produced by a designated security system or security protection operation must individually meet the statutory definition. *Rogers v. Dept. of Rehab. & Corr.,* 155 Ohio St.3d 545, 2018-Ohio-5111, 122 N.E.3d 1208, ¶ 15-21; *State ex rel. Miller v. Pinkney*, 149 Ohio St.3d 662, 2017-Ohio-1335, 77 N.E.3d 915, ¶ 1-4; *Shaffer v. Budish*, Ct. of Cl. No. 2017-00690PQ, 2018-Ohio-1539, ¶ 21-24.

{¶21} The standard of proof is strictly applied against the public records custodian. *Rogers* at ¶ 7. "As we made clear in *Plunderbund*, every record claimed under the security-record exception to disclosure must be considered separately." *Id.* at ¶ 21.

> Unless it is otherwise obvious from the content of the record, the proponent invoking the security-record exemption under R.C. 149.433(A)(1) must provide evidence establishing that the record clearly contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage.

Welsh-Huggins v. Jefferson Cty. Prosecutor's Office, 163 Ohio St.3d 337, 2020-Ohio-5371, 170 N.E.3d 768, ¶ 51. Such evidence is often provided through fact and expert testimony establishing that the records meet the statutory elements. In *Plunderbund*, respondent provided the detailed testimony of several law-enforcement and telecommunications experts connecting the disclosure of the requested information to future risks. *Welsh-Huggins* at ¶ 52, *Plunderbund* at ¶ 22-31.

{¶22} Supporting affidavits must be evaluated for their sufficiency in proving the exemption for each record claimed. In *Rogers*, the Court found on review that

> DRC has not met its burden to show that the requested video falls squarely within the security-record exception codified in R.C. 149.433(B). * * * Here, DRC has provided only two affidavits, one of which merely concludes that "it is [DRC] policy that security videos within correction institutions are not public records, and are therefore not disclosed in response to public records requests." Bobby's affidavit contains more information regarding the applicability of the exception, yet even his testimony is general and insufficient to meet DRC's burden in this case. Beyond these bare allegations, DRC has not attempted to explain how the video recording at issue actually constitutes "information directly used for protecting or

> maintaining the security of a public office against attack, interference, or sabotage," or was "assembled, prepared, or maintained by a public office * * * to prevent, mitigate, or respond to acts of terrorism." R.C. 149.433(A)(1) and (2).

Rogers at ¶ 19.

Certain Requested Data Would Facilitate Interference

{¶23} ODJFS argues that the information it withheld could be used to breach the security of the Dashboard, which is itself designed and used to protect the security of the office's Unemployment Insurance Program from attack, interference, or sabotage. (Response at 11-14; Sur-reply at 5-6.) ODJFS provides the court with affidavits containing at least somewhat more than bare assertions that particular items are security records. ODJFS asserts that the withheld records "*include* what is effectively a 'user guide' for the Google Fraud Software: the Technical Design Document." (Emphasis *sic*.) (Response at 13), arguing that this information would enable bad actors to craft fraudulent applications more likely to elude detection. As noted earlier, ODJFS attests that disclosure of Dashboard information could be expected to have a serious adverse effect on organizational operations, including a significant degradation in mission capability to an extent and duration that the organization is still able to perform its primary functions, but the effectiveness of those functions is significantly reduced. (Sur-reply, Exh. 4 - Supp. Sines Aff. at ¶ 5-13.) The evidence offered by ODJFS thus supports, minimally but sufficiently, that the indicator, flag, weight, and "user manual" records fall squarely within the security records exemption.

Weekly Updates

{¶24} ODJFS withheld portions of seven one-page weekly updates. (Respondent's Jan. 11, 2023 Explanatory Pleading at 13-18.) ODJFS offers no explanation as to how disclosure of redacted portions of the updates meets the statutory definition of a "security record" other than that some contain labels of certain "flags" used in the Dashboard. On review in camera, each update consists of comments presented in three columns; Achievements/Key Updates, Upcoming Activities, and Issue/Risks and Mitigation. The weekly reports contain no algorithms. The bullet-pointed comments consist mainly of the progress status of very generally labeled tasks, generally described needs for permission

or information, the fact that calls/meetings were held or should be held, and reference to "fuzzy logic" that is elsewhere disclosed as a type of processing rather than a specific indicator or flag. The update also contains a Status indication among options of Complete, On Track, Delayed, Behind, or Not Started. The Special Master finds that none of the redacted weekly report information, other than the listed flags, disclose a security record on its face.

{¶25} The Special Master concludes that ODJFS has met its burden to prove that some but not all of the data referenced as security records in the privilege log falls squarely under the exception for "information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage," as identified in the tables at the end of this report.

Trade Secret

{¶26} ODJFS labels some withheld data as trade secret information. The Ohio Uniform Trade Secrets Act defines "trade secret" as:

> information, including the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, pattern, compilation, program, device, method, technique, or improvement, or any business information or plans, financial information, or listing of names, addresses, or telephone numbers, that satisfies both of the following:
>
> (1) It derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
>
> (2) It is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

R.C. 1333.61(D).

{¶27} Like the infrastructure and security record exemption, this is not a "name-it-and-claim-it" exemption but must be proven with evidence showing that the information falls squarely within the full definition of trade secret. "An entity claiming trade secret status bears the burden to *identify* and *demonstrate* that the material is included in categories of protected information under the statute and additionally must take some active steps to maintain its secrecy." (Emphasis added.) *Besser II*, 89 Ohio St.3d 396, 400, 2000-Ohio-207, 732 N.E.2d 373 (2000). To meet its burden, the entity must provide

more than conclusory statements in affidavits to show which, if any, information is a "trade secret." *Id.* at 400-404. Accord *Hance v. Cleveland Clinic*, 2021-Ohio-1493, 172 N.E.3d 478, ¶ 27-32 (8th Dist.); *Harris v. Belvoir Energy, Inc*., 8th Dist. Cuyahoga No. 103460, 2017-Ohio-2851, ¶ 16. The following factors are used by Ohio courts in trade secret analysis:

> (1) The extent to which the information is known outside the business; (2) the extent to which it is known to those inside the business, i.e., by the employees; (3) the precautions taken by the holder of the trade secret to guard the secrecy of the information; (4) the savings effected and the value to the holder in having the information as against competitors; (5) the amount of effort or money expended in obtaining and developing the information; and (6) the amount of time and expense it would take for others to acquire and duplicate the information.

Besser II at 399-400.

{¶28} ODJFS does not claim information as its own trade secret, stating only that "Google asked ODJFS to redact several portions of the [TDD] as trade secrets." (Response at 6, fn. 3.) Further and fatally, ODJFS has not submitted any testimony from Google identifying any particular information as a trade secret, much less demonstrating by evidence that it satisfies the *Besser II* factors. Instead, ODJFS offers only a vague assertion that "it is industry-standard to consider data algorithms as 'trade secrets' or 'intellectual property' and to work hard to protect these algorithms as part of their business." (Sur-reply at 4, Sines Aff. II at ¶ 16.) Even accepting this assertion *arguendo*, ODJFS does not label any specific item in the records as a "data algorithm." In the absence of informed evidence from the putative holder of any trade secret, none of the redacted portions of the records self-identify as data algorithms. Nor are any of the *Besser II* factors demonstrated on the face of the records.

{¶29} The Special Master finds that ODJFS has failed to meet its burden to prove that any of the withheld records falls squarely within the trade secret exemption.

Legend for Exemption Tables:

- *Not claimed* – ODJFS has not asserted the exemption for the listed item
- *Not proven* – ODJFS submitted no evidence beyond the bare assertion of the exemption, and examination of the item *in camera* does not show that the item falls squarely within the exemption

- *By aff.* – affidavit testimony persuades the Special Master at least minimally that the item falls squarely within the exemption
- *By exam* – on examination *in camera* the Special Master finds that application of the exemption is self-evident

Items that are found not to meet the statutory definition of any exemption and must be disclosed are highlighted in **bold underline**.

Technical Design Document (TDD)

Page(s)	Section	Infrastructure (Infr.) or Security (Sec.) Record	Trade Secret
2	**Contents**	**Not proven**	**Not proven**
5	High Level Architecture	Infr. by aff. & exam, Sec. not proven	Not proven
6-7	Flags and Thresholds	Infr. and Sec. by aff & exam	Not proven
7-9	Data Sources & Storage	Infr. by aff. & exam, Sec by aff.	Not claimed
10-12	Data Ingestion & Loading	Infr. by aff. & exam, Sec by aff.	Not claimed
13	Data Processing Workflow	Infr. by aff. & exam, Sec by aff.	Not claimed
13	Data Processing and Flag Score Generation	Infr. by aff. & exam, Sec by aff.	Not proven
13	Fuzzy Logic Processing	Infr. by aff. & exam, Sec by aff.	Not proven
14	Fuzzy Logic Processing	Infr. by aff. & exam, Sec by aff.	Not claimed
15	Fuzzy Logic Processing	Infr. by aff. & exam, Sec by aff.	Not proven
16-17	Fuzzy Logic Processing	Infr. by aff. & exam, Sec by aff.	Not claimed
18-19	Flag Generator or Score Computation	Infr. by aff. & exam, Sec by aff.	Not claimed
20	BigQuery	Infr. by aff. & exam, Sec by aff.	Not proven
20-21	Existing Data Sets	Infr. by aff. & exam, Sec by aff.	Not claimed
21-22	Data Studio Dashboards	Infr. by aff. & exam, Sec by aff.	Not proven
23	Data Studio Dashboards	Infr. by aff. & exam, Sec by aff.	Not proven
23	Fraud Analysis Dashboard Filters - Program	Infr. by aff. & exam, Sec by aff.	Not proven
23	Fraud Analysis Dashboard Filters – Flag Bucket	Infr. by aff. & exam, Sec by aff.	Not claimed
24-25	Fraud Analysis Dashboard Filters – Total Payments	Infr. by aff. & exam, Sec by aff.	Not claimed
25	Managed Data Sources	Infr. by aff. & exam, Sec by aff.	Not proven

26	Managed Data Sources	Infr. by aff. & exam, Sec by aff.	Not proven
27	Linked Fields	Infr. by aff. & exam, Sec by aff.	Not proven
28	Linked Fields	Infr. by aff. & exam, Sec by aff.	Not claimed
29-37	Infrastructure Configuration and Setup	Infr. by aff. & exam, Sec by aff.	Not claimed

Weekly Status Report Emails

Pages	Email	Infrastructure/Security	Trade Secret
49-53	May 13, 2021	Infr. by aff. & exam, Sec by aff.	Not proven
54-57	**May 13, 2021 - Attachment**	**Not claimed**	**Not proven**

Weekly Status Reports

Primary pagination in this table is to *Respondent's Jan. 11, 2023 Explanatory Pleading*. Pagination for the unredacted documents under seal is in parentheses. Pages 14, 15, & 17 contain some permissible exemptions, as noted by table cell text without emphases.

Page	Report Date	Infrastructure/Security	Trade Secret
13 (65)	May 17, 2021	Flags are infrastructure/security records.	Not claimed
14 (66)	May 10, 2021	Flags are infrastructure/security records. **Exemptions not proven for bullet point 2 or for processing term in bullet point 1**	**Not claimed**
15 (67)	May 3, 2021	Flags are infrastructure/security records **Exemptions not proven for Issue/Risk text**	**Not claimed**
16 (68)	**Apr. 26, 2021**	**No exemption proven**	**Not claimed**
17 (69)	Apr. 19, 2021	Issue/Risk text contains infrastructure recds. **No exemption proven for remainder**	**Not claimed**
18 (70)	**Apr. 12, 2021**	**Not proven**	**Not claimed**

Conclusion

{¶30} Accordingly, the Special Master recommends the court order respondent to provide requester with copies of the records and portions of records identified in the Exemption Tables in bold underline as not falling under a proven exemption. It is recommended that costs be assessed to respondent.

{¶31} *Pursuant to R.C. 2743.75(F)(2), either party may file a written objection with the clerk of the Court of Claims of Ohio within seven (7) business days after receiving this report and recommendation. Any objection shall be specific and state with particularity all grounds for the objection. A party shall not assign as error on appeal the court's adoption of any factual findings or legal conclusions in this report and recommendation unless a timely objection was filed thereto. R.C. 2743.75(G)(1).*

JEFF CLARK
Special Master

Filed February 7, 2023
Sent to S.C. Reporter 3/2/23