Case No. 130337

IN THE SUPREME COURT
OF THE STATE OF ILLINOIS

REBECCA PETTA, individually and on behalf of those similarly situated, Plaintiffs-Appellants v. CHRISTIE BUSINESS HOLDINGS COMPANY, P.C. d/b/a CHRISTIE CLINIC Defendant-Appellee.	Petition for Leave to Appeal from the Appellate Court, Fifth District, No. 5-22-0742 Appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, No. 22-LA-51 The Honorable Jason M. Bohm, Judge Presiding

PLAINTIFF-APPELLANT'S BRIEF AND APPENDIX

David M. Cialkowski, IL Bar No. 6255747
Brian C. Gudmundson
Michael J. Laird
Rachel K. Tack
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400

Christopher D. Jennings
JENNINGS PLLC
P.O. Box 25972
Little Rock, AR 72221
Telephone: (501) 247-6267
chris@jenningspllc.com

Counsel for Plaintiff-Appellant Rebecca Petta

ORAL ARGUMENT REQUESTED

E-FILED
Insert text here
5/6/2024 11:12 AM
CYNTHIA A. GRANT
SUPREME COURT CLERK

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

POINTS AND AUTHORITIES

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

NATURE OF CASE

Rebecca Petta ("Petta" or "Plaintiff") appeals an order from the Appellate Court, Fifth District upholding the dismissal of Petta's Complaint, but on different grounds than the trial court's order. Petta brought an action against Christie Business Holding Co., P.C. d/b/a/ Christie Clinic ("Defendant" or "Christie") for harm caused by a data breach during which cybercriminals successfully intruded into Christie's accounts and gained access to patients', including Petta's, highly sensitive personal, health, and insurance information. After the breach, Petta received numerous phone calls concerning multiple attempts to open fraudulent bank accounts using, at the very least, her contact information, but may have also used her social security number, all of which was stolen during the breach. Petta alleged she suffered harm from the misuse of her data and by having to mitigate the significant risk that her information would be used for further fraud and identity theft. She alleges that she faces a prolonged and heightened risk that the cybercriminals who orchestrated the breach will again misuse her data in the future or sell it to other criminals who will do so.

On October 28, 2022, the trial court granted Christie's motion to dismiss Petta's Complaint but rejected its argument that Petta lacked standing. However, the court dismissed her claims for negligence and a violation of the Illinois Personal Information Protection Act, 815 ILCS 530/45(a), for failure to state a claim. Petta appealed the court's order to the Fifth District. On

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

November 28, 2023, the Fifth District upheld the dismissal of Petta's Complaint, reversing the trial court's determination that Petta properly alleged standing and not reaching the merits of her claims.

STATEMENT OF THE ISSUES

1. Whether the theft of a patient's personal and medical information in a data breach constitutes a "cognizable interest" sufficient for standing when the stolen information is used in attempted fraud and identity theft after the breach;

2. Whether a medical provider that collects and stores sensitive personal and medical information owes its patients a common law duty to reasonably safeguard that information when its inadequate data security contributed to a risk of harm, and a data breach and resulting harm to patients was foreseeable, state and federal law already require the defendant to implement reasonable data security, and the burden of imposing such a duty is minimal;

3. Whether the economic loss doctrine is inapplicable where, as here, the duty at issue does not arise in contract, the case presents no risk of limitless liability to unknown plaintiffs and where liability is to a defined group of individuals impacted by a data breach and the plaintiff's harm is not purely economic; and,

4. Whether a plaintiff may assert a claim for a violation of the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) under the Illinois Consumer Fraud Act, 815 ILCS 505/10a(a) for the diminished value of her sensitive personal and medical information.

STANDARD OF REVIEW

The Fifth Circuit reversed the trial court and held Petta's Complaint was properly dismissed because she lacked standing pursuant to Section 2-619 of the Illinois Code of Civil Procedure, and did not reach the trial court's dismissal of Petta's claims pursuant to Section 2-615 of the Illinois Code of Civil Procedure. On appeal, this Court reviews an order granting a motion to

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

dismiss *de novo*. *Kennedy v. City of Chicago*, 2022 IL App (1st) 210492, ¶ 16. When evaluating a motion to dismiss under either Sections 2-615 or 2-619, courts must accept as true all well-pleaded allegations of the complaint and view them in the light most favorable to the plaintiff. *Meerbrev v. Marshall Field & Co.*, 139 Ill. 2d 455, 473, 564 N.E.2d 1222 (1990). The complaint need only "contain sufficient direct or inferential allegations of all material elements to sustain a recovery under some viable legal theory," not exhaustive detail. *Zinser v. Rose*, 245 III. App. 3d 881, 883 (1993).

JURISDICTION

This Court has jurisdiction to hear Petta's appeal under Illinois Supreme Court Rule 315. On January 2, 2024, Petta timely filed her Petition for Leave to Appeal with the Court within 35 days of the Appellate Court's order. On March 27, 2024, the Court granted Petta's Petition.

STATUTES INVOLVED

1. 815 ILCS 530/45(a)

A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

2. 15 U.S.C. § 45(a)(1)

Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

3. 815 ILCS 505/2

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act

4. 815 ILCS 505/10a(a)

Any person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person. The court, in its discretion may award actual economic damages or any other relief which the court deems proper[.] . . . .

5. 815 ILCS 530/10(a)

Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

> (1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of “personal information”:
>
> > (A) the toll-free numbers and addresses for consumer reporting agencies
> >
> > (B) the toll-free number, address, and website address for the Federal Trade Commission; and
> >
> > (C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

> (2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

STATEMENT OF FACTS

I. Christie's Data Breach Exposed Patients' Sensitive Personal and Health Information

Defendant is a physician-owned, multispecialty group that provides medical services throughout Illinois and serves hundreds of thousands of patients. L. R. at C198 V2, ¶¶ 20–22. As a for profit company, Christie secures annual revenues reaching upwards of $132 million. *Id.* at C198 V2, ¶ 21.

As part of its practice, Christie solicits, obtains, and stores patients' personally identifying information, private health and medical information, and insurance information. *Id.* at C198 V2, ¶ 22. With hundreds of thousands of patients seen each year, Christie has built a massive repository of highly sensitive, private information contained within the medical records it collects, creates, and stores. *See id.* at C214 V2, ¶ 82. Christie claims in its privacy policy that "protecting the privacy of healthcare information is a responsibility [it] takes very seriously." *Id.* at C199 V2, ¶ 24. It also represents that "records pertaining to [patients'] care will be treated in confidence" and acknowledges it is required by federal law to "maintain the privacy of [patients'] healthcare information[,]" including requirements established in the federal Health

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Insurance Portability and Accountability Act ("HIPAA"). *Id.* at C198–99 V2, ¶¶ 23–24.

Despite these promises, Christie knowingly implemented deficient data security measures that allowed hackers to: (1) obtain access to a business email account; (2) through that account, access hundreds of thousands of patients' highly sensitive personal, medical, and insurance information; and (3) successfully exfiltrate that information out of Christie control ("Data Breach"). *Id.* at C194 V2, ¶¶ 2–4; C195–96 V2, ¶¶ 6–9; C200–01 V2, ¶¶ 32–35. From at least July 14 to August 19, 2021, the hackers maintained their access to Christie's patients' data, which was sufficient time for them to steal it. *Id.* at C194 V2, ¶ 2; C199 V2, ¶ 28.

After learning of the Data Breach, Christie implemented new data security measures to remedy the deficiencies that led to the Data Breach and warned its patients to take steps to mitigate their risk of harm from fraud and identity theft. *Id.* C195 V2, ¶ 7; C200 V2, ¶ 32. Christie confirmed the Data Breach exposed hundreds of thousands of patients' personal information, including patient names, addresses, social security numbers, medical information, and health insurance information. *Id.* at C200 V2, ¶ 29. This information is widely used by cybercriminals to commit fraud and identity theft and is often sold on the dark web to fraudsters. *Id.* at C201–04, ¶¶ 36–49. Indeed, cybercriminals specifically target medical entities like Christie to obtain this type of sensitive information because of its value on the dark web

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

and its usability for fraud and identity theft. *See id.* at C201 V2, ¶ 36; C205 V2, ¶ 53.

Although the Data Brach compromised highly sensitive personal and medical information, Christie took its time to issue notice to impacted patients. It waited until March 24, 2022, eight months after the Data Breach began, to issue notice to the impacted individuals, including Petta. *Id.* at C200 V2, ¶ 30. Christie's notice to its patients acknowledged the significant risk of fraud and identity theft, and recommended its patients take several time-consuming steps to mitigate these risks. *Id.* at C200 V2, ¶ 32. Christie specifically recommended the Data Breach victims: monitor health and insurance records for services they did not receive and enroll in credit monitoring and identity theft protection services. *Id.*

Plaintiff Rebecca Petta was a Christie patient who received notice that her protected health information was exposed during the Data Breach, including her name, address, social security number, medical information, and health information. *Id.* at C200 V2, ¶ 29. She brought an action against Christie for harm associated with the exposure of her highly sensitive, personal health information, including the actual misuse of her personal information in several fraudulent loan applications. *Id.* at C193–31 V2. Her action was consolidated with another action brought by a Jane Doe plaintiff.[1]

[1] Although the actions were consolidated, they retained a separate identity at the trial court level with each plaintiff having separate complaints. After both Petta and the Doe plaintiff appealed the trial court's order dismissing their

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

After the Data Breach, Petta's stolen information was used several times in attempted fraudulent loan applications. During the period when Christie knew of the Data Breach but did not disclose it, criminals used Petta's stolen personal information to submit multiple fraudulent loan applications at First Financial Bank in Columbus, Ohio (where she does not reside). *Id.* at C197 V2, ¶ 18. Petta does not know the full scope of the information used in those applications but alleged that it at least included her name and address. *Id.* As a result, she had to spend time and effort dealing with the fallout of Christie's Data Breach, including the fake loans, and has taken measures to prevent future harm like monitoring her accounts. *Id.* at C216 V2, ¶ 93. Given that criminals have used her information in fraudulent loan applications, the hackers undoubtedly succeeded in obtaining her private information from Christie during the Data Breach. *Id.* at C197, ¶ 18.

II. The Trial Court's Motion to Dismiss Order

On June 27, 2022, Christie moved to dismiss Petta's complaint. *See id.* at C262 V2. Christie asserted Petta lacked standing, arguing she had not suffered an actionable injury. *Id.* at C272–74 V2. Later, Christie acknowledged in its reply that Petta alleged she suffered attempted fraud, but claimed Petta still lacked standing because those fraud attempts could not be

---

complaints (albeit, for separate reasons), Petta and Doe submitted a joint brief to the Fifth District. While Petta appealed the Fifth District's order, the Doe plaintiff did not seek leave to appeal. Therefore, only the issues raised by Petta's Complaint are at issue here.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

traced to Christie's Data Breach as a matter of fact. *Id.* at C366–67 V2. Christie also asserted all Petta's claims should be dismissed. *Id.* at C273–90 V2. Petta opposed Christie's motion. *Id.* at C291 V2, C323 V2.

On October 28, 2022, the trial court granted Christie's motion to dismiss. *See id.* at C432 V2. The trial court held that Petta properly alleged standing because she reasonably pled that fraudsters had attempted to misuse her information stolen during the Data Breach. *Id.* at C437–38 V2. However, the trial court dismissed Petta's negligence claim and her claim for a violation of the Personal Information Protection Act ("PIPA"). The trial court, relying principally on *Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358 (2010), held that Christie did not have a common law or statutory duty to reasonably safeguard the highly sensitive patient information it collected and stored on its networks and servers. *Id.* at 439–41 V2. The trial court did not evaluate whether the Illinois legislature's recent mandate through PIPA, requiring businesses to reasonably secure personal information, altered *Cooney's* duty analysis set forth a decade earlier.

Notably, although this case does not involve a contract, the duty did not arise in contract, and Petta did not allege any sort of contractual harm, the trial court held that Petta's negligence claim would be barred by the economic loss doctrine. *Id.* at C442–43 V2. Finally, the trial court dismissed Petta's PIPA claim by holding: (1) PIPA does not have a private right of action, even though individuals may bring a claim under the Illinois Consumer Fraud Act

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

("ICFA") for a violation of PIPA; and (2) Petta had not alleged any actual damages. *Id.* at C443 V2. The trial court did not permit Petta to amend her Complaint because it sought guidance concerning standing and Petta's claims from the appellate courts.

III. The Fifth District's Decision Reversing the Trial Court

Petta timely appealed the trial court's dismissal of her Complaint to the Appellate Court, Fifth District. On appeal, she argued the trial court had erroneously held Christie owed her no duty, that the economic loss doctrine applied to her negligence claim, and that she could not assert a claim under PIPA, a violation of which is actionable under the ICFA. Christie opposed Petta's appeal, and reasserted its standing argument, which the trial court had rejected.

The Fifth District upheld the dismissal of Petta's Complaint by reversing the trial court's holding that Petta properly alleged standing. A014–018, ¶¶ 19–29. Although the fraudulent loan applications occurred directly after Christie's Data Breach, involved the same information that Christie admitted was stolen in the Data Breach, and Christie warned Petta that fraud and identity theft might occur after its breach, the Fifth District held the fraud and Data Breach could not be connected. A015–16. ¶ 23. Based on the Fifth District's "quick Google search", it held the fraudulent loan applications could not be fairly traced to the Data Breach because some of Petta's contact information was available online. *Id.* at A016, n.1. The Fifth District, therefore, held that there was "no way in which Petta could, in good faith,

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

allege the loan application activity is 'fairly traceable' back to the defendant's action." *Id.* at A016, ¶ 23. The Court found Petta had no injury caused by Christie's misconduct and, therefore, lacked standing. *Id.* at A017, ¶ 26.

Petta requested leave of this Court to appeal the Fifth District's opinion, which this Court granted on March 27, 2024.

ARGUMENT

Petta appeals the Appellate Court, Fifth District's holding that she lacked standing to bring her claims against Christie arising out of its Data Breach. Additionally, Petta appeals the trial court's order dismissing her negligence and claim under PIPA, which the Fifth District did not reach because it found Petta lacked standing. For the reasons below, this Court should hold: (1) a plaintiff, like Petta, whose information is subject to a Data Breach and subsequently misused and who faces a substantial risk of future harm has suffered an injury in fact for standing purposes; (2) Christie owed Petta a duty to reasonably secure her sensitive personal and medical information under Illinois common law; (3) the economic loss doctrine is inapplicable to Petta's negligence claim; and (4) Petta may bring her claim for a violation of PIPA under the ICFA because she suffered actual damages.

I. PETTA HAS STANDING TO BRING HER CLAIMS AGAINST CHRISTIE

Petta appeals the Appellate Court, Fifth District's reversal of the trial court's determination that she had standing. The trial court held Petta suffered a cognizable injury for standing purposes because, after Christie's

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Data Breach, her personal information was used in several attempted fraudulent loan applications. Although Petta does not know the extent to which her information was misused, at the very least, the fraudulent applications used her name and address, which were involved in Christie's Data Breach, but they may have used more of her information, including her social security number. Nearly every court to have considered the issue has found that alleging attempted fraud or identity theft immediately after a data breach states a sufficient injury for standing purposes.

The Fifth District, however, disagreed with that precedent. Instead, it found Petta's alleged misuse of her information insufficient for standing because she had not definitively proven the information used in the fraudulent loan applications came from Christie's breach. A015–16, ¶ 23.[2] This Court should reverse the Fifth District and hold Petta had standing because: (1) courts overwhelmingly hold that a plaintiff alleges an injury sufficient for standing where, as here, after a data breach, the plaintiff's information was used for fraud or identity theft; (2) the Fifth District's holding that Petta's injuries were not fairly traceable to the data breach was legally deficient because it failed to draw inferences in Petta's favor, imposed a heightened standard for traceability, and improperly held that the fraud was an independent act that undermined traceability; and (3) even absent actual

[2] The full case cite for the Fifth District's opinion, which is included in Petta's Appendix, is: *Petta v. Christie Bus. Holding Co., P.C.*, 2023 IL App (5th) 220742.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

misuse of the stolen data, the threat of future harm is sufficient to establish a cognizable injury.

A. The Theft and Misuse of Petta's Personal Information is an Actual Injury Sufficient for Standing

To establish standing, a plaintiff need only allege an "injury, whether 'actual or threatened'" that is: "(1) 'distinct and palpable'; (2) 'fairly traceable' to the defendant's actions; and (3) substantially likely to be prevented or redressed by the grant of the requested relief." *Greer v. Illinois Housing Dev. Auth.,* 122 Ill. 2d 462, 492–93 (1988) (internal citations omitted). The purpose of the injury requirement is "to preclude persons who have no interest in a controversy from bringing suit." *Glisson v. City of Marion*, 188 Ill. 2d 211, 221 (1999); *see also People ex rel. Hartigan v. E & E Hauling, Inc.*, 153 Ill. 2d 473, 482 (1992) (holding that standing ensures the court considers issues presented by "parties who have a sufficient stake in the outcome of the controversy."). A plaintiff has established that cognizable interest where she alleges "[a] distinct and palpable injury . . . that cannot be characterized as a generalized grievance common to all members of the public." *Illinois Rd. & Transp. Builders Ass'n v. Cnty. of Cook*, 2022 IL 127126, ¶ 17 (internal quotations removed). Conversely, a plaintiff alleging only a "purely speculative" future injury or where there is no "immediate danger of sustaining a direct injury[,]" lacks a sufficient interest to establish standing. *Chicago Teachers Union, Local 1 v. Bd. of Educ. of City of Chicago*, 189 Ill. 2d 200, 207–08 (2000).

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Here, Petta alleged several actual injuries from Christie's inadequate data security and the resulting Data Breach. Specifically, she alleged that her personal and private health information was stolen in the Data Breach, that her stolen information has already been used on fraudulent loan applications, and that she has been required to spend time and effort to mitigate the risk of harm of fraud. L.R. C196 V2, ¶ 11; C197 V2, ¶ 18. The injury alleged is "distinct and palpable," because Petta spent resources attempting to remedy the fraudulent loan applications and because she will be unable to regain the privacy of her personal medical information. Additionally, the data breach is "fairly traceable" to Petta's alleged actual injuries because the misuse of her information occurred in close temporal proximity to when the data was hacked and included the same information impacted by the Data Breach.

Although this Court has not addressed standing in the context of a data breach, both the Illinois Court of Appeals and federal courts have held plaintiffs with similar allegations to Petta have standing. In Illinois, for example, *Flores v. Aon Corp.* held that data breach victims had standing where they "alleged that their personal information has been obtained by unauthorized third parties and that this caused plaintiffs to experience identity theft and fraud." 2023 IL App (1st) 230140, ¶ 15. Similarly, *Maglio v. Advocate Health & Hospitals Corp.* held that data breach victims lacked standing because they had not experienced any fraud or identity theft after the data breach. 2015 IL App (2d) 140782, ¶ 26 (noting plaintiffs lacked standing

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

because they have "not alleged that their personal information has actually been used or that they have been victims of identity theft or fraud[.]").[3]

Furthermore, federal cases have overwhelmingly recognized standing where, as here, the plaintiff alleged fraud or other suspicious activity after a data breach. *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017); *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 373 (1st Cir. 2023) (finding that the complaint "plausibly alleges a concrete injury in fact" because "the data breach resulted in the misuse of her [personally identifying information] by an unauthorized third party (or third parties) to file a fraudulent tax return."); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (finding the use of mitigation measures to safeguard against future identity theft not too speculative to establish standing when a substantial risk of harm actually exists because the data has been misused); *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018) (finding that stolen personal information that had already been used was sufficient to establish standing); *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 888–89 (11th Cir. 2023) (finding an actual injury from stolen credit card information being posted

[3] The Fifth District's decision similarly appears to recognize the misuse of the data from a data breach is sufficient for standing. A011–12, ¶ 14. (holding the Doe plaintiff, who filed a separate action from Petta, lacked standing because she "does not allege that her information has been improperly used or that she has suffered identity theft and/or identity fraud because of the data breach."). Although Petta made such allegations, the Fifth District improperly disregarded them, demanding Petta establish a definitive causal connection between the Data Breach and fraud. As described further below, that holding was erroneous.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

on the dark web conferred standing). In fact, federal courts have found that the risk of harm alone, even without definitive misuse of data, suffices to establish standing. *See, e.g.*, *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155-156 (3d Cir. 2022) (holding "[c]ourts also consider whether the data was misused" but noting "misuse is not necessarily required" and courts "ha[ve] found standing despite no allegations of misuse[.]").

This precedent fully supports Petta's standing here. Although federal law is not binding, Illinois generally considers its standing requirements to be more liberal than those of federal courts. *See Greer*, 122 Ill. 2d at 491 ("[T]o the extent that the State law of standing varies from Federal law, it tends to vary in the direction of greater liberality[.]"); *Flores*, 2023 IL App (1st) 230140, ¶ 13 ("Illinois courts are generally more willing than federal courts to recognize standing on the part of any person 'who shows that he is in fact aggrieved.'" (citing *Greer*, 122 Ill. 2d at 491)). Since Petta's alleged harm—the express misuse of her personal information stolen in Christie's breach—is sufficient to establish standing under federal law, the Court should hold it is a sufficient injury in fact here.

B. The Fifth District Erroneously Held the Misuse of Petta's Information Was Not "Fairly Traceable" to Christie's Breach

For standing, Illinois law requires that the plaintiff's alleged injury be "fairly traceable to the defendant's actions[.]" *Greer*, 122 Ill. 2d at 493. Although the Fifth District acknowledged Petta alleged the information stolen

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

in the Data Breach was used in fraudulent loan applications, it found Petta had not sufficiently linked the breach and the fraud because the fraudsters could have obtained her information is online. A015–16, ¶¶ 22 – 23, n.1.

The Court should reverse the Fifth District's determination because it erroneously analyzed the traceability requirement. Specifically, the Fifth District: (1) failed to accept Petta's allegations as true or draw inferences in her favor; (2) improperly imposed a heightened standard of traceability beyond that of legal causation; and (3) held, contrary to the law, that an intervening act by a third party upends traceability. For the reasons explained below, the Court should hold Petta has established standing at this stage.

1. The Fifth District Failed to Draw Inferences in Petta's Favor

In holding Petta lacked standing, the Fifth District's opinion improperly construed the Complaint, drawing inferences in Christie's favor and evaluating facts outside the four corners of the complaint. When inferences are drawn in Petta's favor, as they should be at this stage, her allegations sufficiently connect the Data Breach and resulting fraud.

"[A] plaintiff's lack of standing is an affirmative defense and, as such, must be pleaded and proven by the defendant." *Maglio*, 2015 IL App (2d) 140782, ¶ 21. In ruling on a motion dismiss for lack of standing, "the court must interpret the pleadings and supporting materials in the light most favorable to the nonmoving party." *Id.* "Where standing is challenged by way of a motion to dismiss, a court must accept as true all well-pleaded facts in the

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

plaintiff's complaint and all inferences that can reasonably be drawn in the plaintiff's favor." *Int'l Union of Operating Eng'rs, Local 148, AFL-CIO v. Illinois Dep't of Emp. Sec.*, 215 Ill. 2d 37, 45 (2005). "Whether the plaintiff has standing to sue is to be determined from the allegations contained in the complaint." *Martini v.* Netsch, 272 Ill. App. 3d 693, 670 (1995) (citing *People ex. rel. Lee v. Kenroy, Inc.*, 54 Ill App. 3d 688, 692 (1977)).

Here, the Fifth District drew inferences not in Petta's favor, but instead, made significant assumptions in Christie's favor. The Court acknowledged Petta's personal information had been used in several fraudulent loan applications directly after the Data Breach, and that prior case law would find standing in such circumstances. A011–12, ¶ 14. However, the Fifth District declined to find Petta had standing because it believed "there [was] no apparent connection between the purported fraudulent loan attempt and the data breach." A015–16, ¶ 23. The court based its holding on a google search it conducted that supposedly identified some of Petta's contact information online, which the court then held may have been the source of information in the fraudulent loan applications. *Id.*

The Fifth District's analysis ignored the allegations in Petta's Complaint connecting the fraud and the Data Breach. To find that Petta's injuries were not traceable to the Data Breach, the Fifth District erroneously assumed that ***only*** Petta's contact information was used on the fraudulent loan applications. However, Petta did not allege that the loans were limited to using her contact

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

information. While Petta knows one loan used at least her name and address, she received "multiple phone calls . . . regarding loan applications she did not initiate" after the Data Breach, and she was not told what of her information was used in those other loan applications. L.R. C197 V2, ¶ 18.

Drawing inferences in her favor, as is required at the stage, supports the view that the fraudulent loan applications occurring directly after the Data Breach and using some of the same information stolen in the Data Breach occurred due to that breach. Indeed, Christie's notice of the data breach expressly warned Petta and its other patients of the possibility of fraud from the breach. L.R. C200 V2, ¶ 32. Moreover, Christie admitted social security numbers were impacted by the Data Breach and, given that loan applications require such information, it is reasonable to infer Petta's other data, such as her social security number, was also misused.[4] *Id.* at C197 V2, ¶ 29; *see also Portier v. NEO Tech. Sols.*, No. 3:17-cv-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) (describing theft of a social security number as the "gold standard" for standing).

[4] The Fifth District appears to have believed it that would be impossible to prove the fraud occurred due to the Data Breach without testimony from the fraudsters. A015–16, ¶ 23. Circumstantial evidence, however, can do the job. For instance, Petta may show, through discovery, that her social security number was used in the fraudulent loan applications and there is no other known source of exposure of her social security number. In short, the Fifth District's view that only direct evidence will suffice to reasonably establish causation ignores other sources of evidence and would, more critically, doom essentially all data breach actions because fraudsters generally do not make themselves available for discovery.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Finally, the Fifth District also went well beyond the boundaries of the Complaint to construct its traceability argument. *Martini*, 272 Ill. App. 3d at 670. In rejecting traceability, the Fifth District performed its own google search to look for Petta's information online, and then concluded it was likely the fraudsters used Petta's information out of tens of millions of others listed online. A fact dispute as to the source of the misused information should not, and cannot, be resolved on a motion to dismiss. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 467 (D. Md. 2020). ("While [d]efendant[] may ultimate show, after the opportunity for discovery, that the alleged injuries are not caused by their data breach, it is premature to dismiss [p]laintiffs' claims on grounds of traceability.").

The Court should therefore reject the Fifth District's traceability holding and find Petta properly alleged standing.

2. The Fifth District Imposed a Heightened Standard for Traceability

In addition to improperly drawing inferences in favor of Christie, the Fifth District also improperly imposed a heightened traceability standard at the pleading stage. Illinois borrowed its requirement that an injury be "fairly traceable" to the defendant's wrongdoing from federal law. *See Greer*, 122 IL 2d at 493 (citing *Village of Arlington Heights v. Metro. Housing Dev. Corp.*, 429 U.S. 252, 261 (1977)). In federal court, especially at the pleading stage, the "fairly traceable" requirement is a low burden. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) ("A showing that an injury is 'fairly traceable

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

requires less than a showing of proximate cause." (internal quotations omitted)); *Toretto v. Donnelley Fin. Sols., Inc.*, 523 F. Supp. 3d 464, 472 (S.D.N.Y. 2021) ("[P]articularly at the pleading stage, the 'fairly traceable' standard is not equivalent to a requirement of tort causation" and "we are concerned with something less than the concept of proximate cause." (emphasis removed)). Generally, "fairly traceable" means "more than speculative but less than but-for." *Parsons v. U.S. Dep't of Justice*, 801 F.3d 701, 714 (6th Cir. 2015).

Here, the Fifth District held Petta to an impossible standard of proof for traceability at the pleading stage. The court held Petta cannot "in good faith" allege traceability because, in the court's view, "[t]here's no way, outside of speculating" to connect the Data Breach and the subsequent fraud. A015–16, ¶ 23. It supports its view by noting that the "independent hackers who are responsible for this data breach . . . are not before the court." *Id.*

Under such a view, it would be impossible in any action to ever connect fraud or identity theft because the fraudsters are never before the court. The Fifth District's requirement of definitive proof, thus, not only exceeds the traceability standard, it upends the standard for establishing causation in tort where circumstantial evidence is often used to establish causation. *See Berke v. Manilow*, 2016 IL App (1st) 150397, ¶ 35 ("The plaintiff may establish proximate cause through circumstantial evidence. That is, causation may be established by facts and circumstances that, in the light of ordinary experience,

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

reasonably suggest that the defendant's negligence operated to produce injury." (internal citations removed)).

Indeed, most courts examining traceability in the context of a data breach case rely on circumstantial factors to determine standing, including the proximity between the breach and fraud and whether the type of information impacted by the data breach can be used to orchestrate fraud. *See, e.g.*, *In re Mednax Srvs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1205–06 (S.D. Fla. 2022) (finding traceability satisfied where "the [d]ata [b]reaches occurred, whereby unauthorized persons gained access to [p]laintiffs' private information" and "[f]ollowing the [d]ata [b]reaches, [p]laintiffs experienced documented incidents of identity theft[.]"); *Marriott*, 440 F. Supp. 3d at 466–67; *Resnick*, 693 F.3d at 1324.

Here, the circumstantial factors support Petta's allegations connecting the fraud and the Data Breach. Christie admitted that Petta's contact information and social security number we impacted by the Data Breach, both of which can be used to submit fraudulent loans applications. Additionally, the fraud occurred directly after the Data Breach, suggesting they are likely related. *See S. Indep. Bank v. Fred's, Inc.*, No. 2:15-cv-0799, 2019 WL 1179396, at *8 (M.D. Ala. Mar. 13, 2019) ("It is nothing more than common sense to say that when two unique events known to bear a causal relationship—a data breach and subsequent fraudulent transaction—occur in the same limited time frame, there is a higher probability that the former caused the later."). As

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

such, Petta's allegations are sufficient at this stage to connect the fraud and the Data Breach. The Court should find she properly alleged standing.

3. An Intervening Act Does Not Negate Traceability

Finally, the Fifth District incorrectly decided that an injury could not be "fairly traceable" if it is the "product of some independent action taken by a third party that is not before this court[5]." A016, ¶ 23. Since the fraud was committed by criminals, the Fifth District held that the action of the hackers constituted an "independent action" that negates traceability. *Id.* This Court should reject that view.

As other courts have held, a defendant need not be the most immediate cause or the proximate cause of the injury for the injury to be "fairly traceable" to the defendant. *Attias*, 865 F.3d at 629; *see also Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 695 (7th Cir. 2015) (finding the fact that another store "*might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue" because it is "certainly plausible for pleading purposes that their injuries are 'fairly traceable'" to the

[5] The standard adopted by the Fifth District is stricter than the standard applied by other appellate courts in Illinois. In *Maglio*, the Second District held that the plaintiffs had no standing because none of them alleged any "identity theft ha[d] occurred to any of the[m]." 2015 Ill. App. (2d) 140782, at ¶ 25. The plaintiffs in *Maglio* only alleged that they were at increased risk. *Id.* Similarly, in *Flores*, the First District adopted a less stringent standard when it found that because plaintiffs had "already experienced fraudulent charges and spam messaging" they had "clearly alleged that they face imminent, certainly impending, or a substantial risk of harm." 2023 IL App (1st) 230140, at *3. The court also found the defendants offering of free credit monitoring supported allegations of a risk of future harm. 2023 IL App (1st) 230140, at *3.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

data breach at issue) (emphasis in original, citation omitted)). Indeed, "[e]ven a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement." *Resnick*, 693 F.3d at 1324.

Similarly, in Illinois, defendants can be liable for harm committed by third party criminals where they contribute to the risk of harm. *See, e.g.*, *Fancil v. Q.S.E. Foods, Inc.*, 60 Ill. 2d 552, 555 (1975) ("An act or omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal." (quoting Restatement (Second) of Torts § 302(b)).

Most courts recognize that subsequent fraud or identity theft solidifies standing, rather than undermining it. *See Attias*, 865 F.3d at 627 ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."). The Fifth District's view, however, would mean that subsequent fraud or misuse of data absolves those whose inadequate security caused the theft of that data in the first place. That would contradict the very purpose of requiring reasonable data security—to prevent the theft and misuse of personal information. *See, e.g.*, 815 ILCS 530/45(a) (requiring "reasonable security measures to protect . . . records from" among other things, "unauthorized access" and "use[.]"). Here, Christie's unreasonable data security put Petta at risk, resulted in a Data Breach, and is

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

reasonably alleged to have caused fraudulent transactions with Petta's information. That is sufficient for standing.

C. The Threat of Future Harm is Separately Sufficient to Establish Petta's Standing

Although Petta alleged an actual injury due to the misuse of her personal information for attempted fraud, Petta would separately have standing to bring her claims due to the substantial risk of harm she faces given that her data is knowingly in the hands of cybercriminals.

In *Greer*, this Court noted that the threat of a future injury can suffice to establish standing, at least where plaintiffs seek declaratory and injunctive relief. 122 Ill. 2d at 494 ("While at the time the complaint was brought this injury was 'threatened' rather than actual, the lack of immediate, ascertainable damages is not itself a barrier to the grant of declaratory or injunctive relief."). Given the imminent threat of fraud and identity theft posed by certain data breaches, courts have similarly held that a substantial threat of future injury can establish standing. *See Clemens*, 48 F.4th at 153 (holding "misuse [of the data] is not necessarily required" for standing); *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. App'x 384, 388 (6th Cir. 2016) ("There is no need for speculation [about an injury] where [p]laintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for fraudulent purposes[.]").

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

When considering whether a data breach poses a "substantial risk of harm", courts have looked at three factors, including whether: (1) the data breach was intentional; (2) the data subject to the breach has been misused; and (3) the data is capable of being used for fraud or identity theft. *Clemens*, 48 F.4th at 153–54; *see also In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1254–55 (M.D. Fla. 2019). Here, each of those factors support finding a substantial risk of harm and, as such, standing.

First, Petta alleged that the cybercriminals purposely targeted Christie because of the value of its repository of patient data. L.R. C214 V2, ¶ 82. Further, she alleged that the cybercriminals succeeded in taking swaths of private medical information on hundreds of thousands of patients. *Id.* at C196 V2, ¶ 9.

Second, Petta further alleges that her information has been misused, indicating that she faces a risk of continued misuse of her data because it is in the hands of fraudsters. L.R. C197 V2, ¶ 18. Even if only her personal information was used in the fraudulent loan attempts, the fraudsters' access to that personal information suggests they also acquired the other information impacted by the Data Breach, including her social security number and medical and health information. *Id.* at C200 V2 ¶ 29. Further establishing the risk of misuse, Christie recommended Petta take remedial and mitigatory measures to prevent future fraud and identity theft. *Id.* at C200 V2, ¶ 32; *see also Flores*, 2023 IL App (1st) 230140, ¶ 15 ("[T]he risk of future identity theft

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

and fraud is evident from the defendant's statements" and its offer of "free enrollment in a two-year credit-monitoring service to protect against identity theft.").

Third, as Christie admits, the Data Breach exposed patient names, addresses, social security numbers, and medical and health information. *Id.* at C200 V2, ¶ 29. "[D]isclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud." *Clemens*, 48 F.4th at 154. Indeed, "[b]ecause social security numbers are the gold standard for identity theft, their theft is significant." *Portier*, 2019 WL 7946103, at *12.

Collectively, these factors establish that Petta remains at a heightened risk of future harm which justifies the mitigatory measures she has taken and suffices to establish standing.

II. ILLINOIS' TRADITIONAL NEGLIGENCE PRINCIPLES SUPPORT A DUTY TO REASONABLY SECURE SENSITIVE INFORMATION

Petta asserted a negligence claim against Christie, alleging it breached a duty to her and other patients to reasonably secure their personal and private medical information against the reasonably foreseeable threat of a cyberattack. The Fifth District did not reach the issue of Christie's duty, instead upholding the trial court's dismissal of Petta's Complaint by reversing the trial court's decision on standing. However, the Court here should revive Petta's negligence claim and find Christie owed her a duty under the common law.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

The existence of Christie's duty is guided by Illinois's traditional negligence principles, which proceed through two steps: (1) a threshold inquiry of whether the defendant's own acts and omissions contributed to the risk of harm; and (2) if so, an evaluation of four public policy factors for evaluating duty that consider, among other things, the foreseeability and likelihood of the injury and the impact of placing a duty on the defendant.

Here, as explained further below, this Court should hold Christie owed Petta a duty. First, as other courts have found in other similar data breach cases, Christie's own acts and omissions, specifically, its collection and storage of sensitive information and inadequate data security, contributed to the risk of a data breach. Second, the four public policy considerations support Christie's duty because the Data Breach and Petta's harm were foreseeable and Christie, as the only entity capable of securing Petta's information, is already obligated by state and federal law to implement reasonable data security.

A. Petta Satisfied the Threshold Inquiry Because She Alleged Christie's Own Acts and Omissions Contributed to the Risk of Harm

"Where [a] plaintiff seeks recovery based on the defendant's alleged negligence, the plaintiff must plead and prove the existence of a duty owed by the defendant, a breach of that duty, and injury proximately resulting from that breach." *Bogenberger v. Pi Kappa Alpha Corp., Inc.*, 2018 IL 120951 (2018), ¶ 21. "Whether a duty exists is a question of law for the court to decide."

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Id. (citing *Forsythe v. Clark USA, Inc.*, 224 Ill. 2d 274, 280, 309 Ill. Dec. 361 (2007)). Here, Petta contends Christie owed her a duty due to reasonably secure the personal information Christie collected and stored.

Before assessing whether Christie owed Petta duty, Illinois courts consider a threshold inquiry necessary to determine which standard governs the analysis. As this Court has explained, "the duty analysis must begin with the threshold question of whether the defendant, by his act or omission, contributed to a risk of harm to this particular plaintiff." *Simpkins v. CSX Transp., Inc.*, 2012 IL 110662, ¶ 21; *see also Bogenberger*, 2018 IL 120951, ¶ 69 (J. Theis, concurring). "If the answer to that question is yes, . . . [then] [t]he court must weigh the public policy considerations[.]" *Bogenberger*, 2018 IL 120951, ¶ 69. Those public policy considerations include four factors: (1) the foreseeability of the injury; (2) the likelihood of the injury given the defendant's negligence; (3) the magnitude of the burden of guarding against the injury; and (4) the consequences of placing that burden upon the defendant. *Ward v. K Mart Corp.*, 136 Ill. 2d 132, 140–41 (1990). If "the answer to that threshold question is no, the analysis shifts" and "[t]he court must look to a so-called 'special relationship' that establishes an [affirmative] duty." *Id.*

Here, Petta alleged Christie's own acts and omissions contributed to the risk of harm from a data breach. Specifically, Petta alleged Christie collected and stored highly sensitive patient information, including medical information. L.R. C200 V2 ¶ 33, C214 V2, ¶ 82. She further alleged Christie

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

used knowingly inadequate data security to protect it, as evidenced by: (1) the cybercriminals' lengthy access to Christie's system, indicating its data security failed to detect the intrusion; (2) the number of patients' whose information was impacted (over 500,000); (3) the significance of the information exposed (including social security numbers, medical information, and health insurance information), which are prime targets for cybercriminals; and (4) the cybercriminals' success in obtaining patient information, including Petta's, which they subsequently used to attempt fraud.[6] L.R. C194 V2, ¶ 2, C197 V2, ¶ 18, C200, ¶¶ 29, 34–35.

Although no Illinois court has considered the threshold inquiry in assessing duty in a data breach case, courts in other jurisdictions have held entities that collect and store sensitive information and implement inadequate data security contribute to the risk of harm. In *In re Netgain Technol., LLC*, for example, the United States District Court for the District of Minnesota considered that question in the context of Minnesota's negligence principles,

[6] Although Petta does not plead Christie's data security deficiencies in exacting detail, courts have recognized the "unique challenges for plaintiffs at the pleading stage" because plaintiffs "may know only what the company has disclosed in its notice of a data breach" and defendants have "good reasons . . . to keep the details of its security procedures and vulnerabilities private from the public and other cybercriminal groups." *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1220 (11th Cir. 2023). Thus, courts "cannot expect a plaintiff . . . to plead with exacting detail every aspect of [a defendant's] security history and procedures that might make a data breach foreseeable[.]" *Id.* At this stage, Petta has adequately alleged that Christie inadequately protected patient data.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

which closely mirror Illinois's. No. 21-cv-1210, 2022 WL 1810606, at *10–11 (D. Minn. June 2, 2022). The *Netgain* Court agreed with the plaintiffs there that "this [was] not a special relationship case, but rather a general negligence case where Netgain's own conduct, in failing to maintain appropriate data security measures, created a foreseeable risk of harm that occurred[.]" *Id.* at *11. The *Netgain* court, thus, went on to consider Minnesota's four duty factors—which are similar to Illinois's public policy considerations—and found the defendant owed plaintiffs a duty. *See id.* (finding a duty because "[s]imply put, [p]laintiffs allege[d] that Netgain's own conduct created a foreseeable risk of injury to a foreseeable plaintiff." (internal quotations omitted)).[7]

Here, Petta alleged that Christie collected patient information and implemented knowingly inadequate data security. At this stage, those

[7] Many other courts have agreed that an entity who gathers and stores sensitive information contributes to the risk of harm by using knowingly inadequate data security. *See, e.g.*, *Dittman v. UPMC*, 649 Pa. 496, 512–13 (Pa. 2018) (holding, under Pennsylvania law, that "this case is one involving application of an existing duty to a novel factual scenario, as opposed to the imposition of a new, affirmative duty" and "[plaintiffs] have sufficiently alleged that [defendant's] affirmative conduct created the risk of a data breach." (quotations and citation omitted)); *In re Brinker Data Incident Litig.*, No. 3:18-cv-0686, 2020 WL 691848, at *7 (M.D. Fla. Jan. 27, 2020) (holding, under Florida law, that "[t]he acts here are acts of commission, which historically generate a broader umbrella of tort liability" and "the commission was the alleged negligent collection and storage of personal information and payment card data.") (quotations omitted)); *In re Sonic Corp. Customer Data Sec. Breach Litig.*, No. 1:17-md-2807, 2020 WL 3577341, at *3 (N.D. Ohio July 1, 2020) (holding, under Oklahoma's more stringent duty standard, that the defendant had a duty to use reasonable data security because its "affirmative acts exposed [p]laintiffs to a high degree of risk which a reasonable person would have considered.").

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

allegations are sufficient to establish that Christie contributed the risk of a data breach, a risk that ultimately materialized and caused injury to Petta. Based on that threshold inquiry, whether Christie owed a duty is governed by the public policy factors rather than the "special relationship" test.

B. Illinois' Public Policy Factors Each Support Finding Christie Owed Petta a Duty

Because Christie's conduct satisfies the threshold inquiry, the Court looks to the public policy factors to determine if Christie owed a duty to Petta. As described below, each of those factors support a finding of duty here. The public policy considerations include: (1) the foreseeability of the injury; (2) the likelihood of the injury given the defendant's negligence; (3) the magnitude of the burden of guarding against the injury; and (4) the consequences of placing that burden upon the defendant.[8] *Ward*, 136 Ill. 2d at 140–41. "[T]he weight accorded [to] each of these factors in any given analysis depends on the circumstances of the case at hand." *Simpkins*, 2012 IL 110662, ¶ 18.

As described below, the public policy factors each fully support finding Christie owed a duty. In similar cases, courts evaluating these factors have determined they support finding entities storing sensitive data have a duty reasonably secure that data. *See Flores*, 2023 IL App (1st) 230140, ¶ 24 ("All

[8] Although these factors are sometimes described as factors evaluating the "relationship" between the parties, the "relationship" requirement simply "acts as a shorthand description for the sum of [the] four [public policy] factors" and an "independent 'direct relationship' between the parties . . . is not an additional requirement to establishing a duty[.]" *Simpkins*, 2012 IL 110662, ¶ 18–19.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

four factors support the conclusion that defendant has a common law duty to protect the personal information of its clients[.]"); *Marriott*, 440 F. Supp. 3d at 478 (evaluating the public policy considerations and holding that "[t]hese allegations do suggest that an Illinois court could find a duty" but leaving it to "the Illinois Supreme Court . . . to consider this issue, along with the application of the economic loss rule to data breach cases.").

Here, as the *Flores* court found and as described further below, the public policy factors fully support finding a duty.

1. Christie's Data Breach and the resulting harm were foreseeable

Petta alleged a foreseeable injury, namely, that because Christie failed to implement adequate data security measures, her information was stolen and misused due to a data breach of a targeted health care entity. *See Ward*, 136 Ill. 2d at 140–41. In describing a reasonably foreseeable injury, this Court has defined what it is not foreseeable: "an injury resulting from . . . freakish, bizarre, or occurring under fantastic circumstances." *Bogenberger*, 2018 IL 120951, ¶ 46 (internal quotations removed).

Here, Petta does not allege a freakish or bizarre injury, but the exact injury expected when sensitive information is taken in a data breach—the misuse of the data for fraud. Petta alleged the misuse of her data and the fallout from the attempted fraud was a highly foreseeable result of Christie's unreasonable data security. Petta alleged Christie collected, created, and stored her highly personal and private information on its own servers,

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

including her personal identifying and medical information. L.R. at C198 V2, ¶¶ 22, 33.

It is common knowledge, especially to medical providers, that medical facilities storing patient information are targeted by hackers because that information can be sold for illicit purposes. *Id.* at C200 V2 ¶ 33; C205 V2, ¶ 53; C214 V2, ¶¶ 81–82. As a prime target for cybercriminals, Christie knew or should have known that inadequate data security measures would likely lead to a data breach that could harm its patients. *Id.* at C205 V2, ¶ 53; C14, ¶ 82. Indeed, acknowledging this risk of harm, Christie told patients it would protect their data and adhere to data security standards required under federal law. *See, e.g.*, *id.* at C199 V2, ¶¶ 25–26; C203–04 V2, ¶¶ 46–49; C208–10 V2, ¶¶ 64–68. Consequently, the risk of a data breach and harm to Christie's patients were a foreseeable result of its inadequate data security.

Additionally, both the *Flores* and *Marriott* courts found data breaches foreseeable where the defendant collected and stored sensitive personal information. *Flores*, 2023 IL App (1st) 230140, ¶ 25; *Marriott*, 440 F. Supp. 3d at 477–78; *see also Netgain*, 2022 WL 1810606, at *10; *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360 (N.D. Ga. 2021) (finding that "as a health care provider, Defendant knew or should have known that it faced a particularly high risk of data breach."). Because his case involves a highly foreseeable cybercriminal attack against a foreseeable target, Christie had a

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

duty to act reasonably to prevent an intrusion on its system and the theft of its patients' information.

2. The likelihood of injury from a data breach is significant

Data breaches also create a well-known, lasting threat to those whose sensitive information was exposed, stolen, especially where subsequently used for fraud. L.R. at C201 V2, ¶ 39; C202 V2, ¶¶ 54–55; C207–08 V2, ¶¶ 58–63. Here, Petta alleged that the Data Breach created a significant risk of harm because the cybercriminals successfully accessed and stole her medical and personal information, allowing them to misuse it. *Id.* at C199–00 V2, at ¶¶ 28–29.

Courts across the country have recognized that data breach victims face a significant risk of harm where, as here, cybercriminals targeted and obtained individuals' sensitive information. *See 21st Century*, 380 F. Supp. 3d at 1254 ("[T]he circuits have found that an increased risk of identity theft is more likely . . . where there is evidence that a third-party has accessed the sensitive information and/or already used the compromised data fraudulently."); *Attias*, 865 F.3d at 628 ("[Defendant] does not seriously dispute that plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were accessed by a network intruder[.]"); *Galaria*, 663 Fed. App'x at 388 ("[A]lthough it might not be 'literally certain' that [p]laintiffs' data will be misused, there is a sufficiently substantial risk of harm . . . . Where [p]laintiffs already know that they have lost control of their data, it would be unreasonable

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

to expect [p]laintiffs to wait for actual misuse[.]"); *Netgain*, 2022 WL 1810606, at *5 ("[T]here is a substantial risk of harm when [personally identifying information] and [personal health information] is stolen.").

As these and numerous other courts have found, data breach victims face a high risk of injury when their sensitive information is targeted, accessed, and taken by criminals. Christie was on notice that its unreasonable data security posed a significant risk to Petta, and that risk materialized when the cybercriminals breached Christie's system, stole Petta's personal information, and either attempted to misuse it or sold it to fraudsters who did.

3. State and Federal law already require Christie to guard against a data breach

The third policy factor considers the burden of guarding against the harm of a data breach, and also supports the Court finding a duty here. *Ward*, 136 Ill. 2d at 140–41. The Court has stated that "[t]here can be no real burden to require [a defendant] . . . to comply with the law and [their own policies.]" *Bogenberger*, 2018 IL 120951, ¶ 46. Here, because Christie was already required by its own patient policy and state and federal law to protect against a data breach, this factor is easily satisfied. *See* L.R. C198–99 V2, ¶¶ 23–24, C199, V2, ¶¶ 24–25.

First, Christie admits federal law required it to implement reasonable security measures. As Petta alleged, Christie represented in its Patient Privacy Policy that the "privacy of healthcare information is a responsibility [it] take[s] very seriously" and it assured patients that they have a right to the

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

privacy and confidentiality of their medical records. L.R. C198–99 V2, ¶¶ 23–24. It also acknowledged its obligations to comply with HIPAA and other federal laws requiring it to take measures to "maintain the privacy of [patients'] information." *Id.* at C199, V2, ¶¶ 24–25.

Second, PIPA requires data collectors like Christie to safeguard personal data:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident *shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.*

815 ILCS 530/45(a) (emphasis added).[9]

Third, under federal law, Christie was required to take measures to "maintain the privacy of [patients'] information." L.R. at C199, V2, ¶¶ 24–25. HIPAA, for example, lists specific technical, administrative, and physical measures that entities like Christie must implement to protect patient

---

[9] At least two courts have found that PIPA, which was amended in 2017 to add a requirement to secure personal information, negates prior case law finding PIPA did not support a duty. *Flores*, 2023 IL App (1st) 230140, ¶ 23; *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, at 590 (N.D. Ill. Sept. 28, 2022). Notably, *Cooney v. Chicago Public Schools* held PIPA did not support a duty to secure personal information because it was decided years prior to the 2017 amendments and, at the time, PIPA "limit[e]d defendants' duty to providing notice" after a data breach occurred. 407 Ill. App. 3d 358, 362 (2010). The *Cooney* Court held that "the creation of a new duty beyond the legislative requirements already in place [in PIPA] [was not] part of [its] role on appellate review." *Id.* at 363. However, since PIPA now requires entities to implement reasonable data security, 815 ILCS § 530/45(a), PIPA supports a duty to implement reasonable data security, rather than detracting from such a duty. *Flores*, 2023 IL App (1st) 230140, ¶ 23.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

information. 45 C.F.R. §§ 164.308, 164.310, 164.312. The Federal Trade Commission ("FTC") also requires entities to enact reasonable data security measures to protect customer information pursuant to 15 U.S.C. § 45(a), which prohibits unfair or deceptive practices in business. *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015) (holding that "companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers" violate the FTC Act).

As such, not only did Christie's own policy already require it to protect Petta's data, but so did state and federal law. Consequently, the burden of requiring Christie to use reasonable data security to prevent a Data Breach is minimal.

4. Only Christie had the ability to protect patient information accessible using its accounts

Fourth and finally, in assessing whether a duty exists, Illinois courts examine the potential consequences of placing the burden of preventing plaintiff's injury on the defendant. *Ward*, 136 Ill. 2d at 140–41. Because Christie was the only entity capable of securing the sensitive information within its possession, this factor also supports finding a duty. Indeed, Christie had sole authority and control over its systems. Courts have placed the responsibility of protecting data on the on the entities soliciting and storing it:

> To hold that no such duty [to safeguard information] existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyberattacks, leaving consumers with no resource to recover damages even though the

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

> retailer was in a superior position to safeguard the public from such a risk.

In re: The Home Depot, Inc., Customer Data Sec. Breach Litig., 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016); *see also Stasi v. Inmediata Health Grp., Corp.*, 501 F. Supp. 3d 898, 915 (S.D. Cal. 2020) (holding that "imposing a common law duty on companies that possess personal and medical information to safeguard that information further promotes a policy, statutorily recognized, of preventing identity theft and protecting the confidentiality of medical information.") For similar reasons, PIPA places the duty to implement reasonable data security measures on the "data collector[s]" who "maintain[] or store[] . . . records that contain personal information[.]" *See* 815 ILCS 530/45(a).

At all times, Christie managed its email accounts, servers, and data security and was the only entity that could protect the patient information it collected and stored. Thus, this factor also supports finding Christie's duty. Because each public policy factor supports finding entities collecting sensitive information owe the subjects of that information a duty, the Court should hold Christie owed Petta such a duty here.

III. THE ECONOMIC LOSS DOCTRINE DOES NOT APPLY TO PLAINTIFF'S NEGLIGENCE CLAIM

The economic loss doctrine, known in Illinois as the *Moorman* doctrine, limits the availability of tort actions in certain cases where the harm is purely economic. *See Moorman Mfg. Co. v. Nat'l Tank Co.*, 91 Ill. 2d 69 (1982). The

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

economic loss doctrine is not intended to be a wholesale ban on the recovery of economic damages in tort. Instead, Illinois applies the doctrine in two circumstances to achieve two specific policy aims: (1) where the duty arises out of contract to prevent plaintiffs from recovering in tort for the breach of contract; and (2) to avoid unbounded liability from attenuated, downstream plaintiffs seeking recovery of economic losses.

Here, the Court should reverse the trial court's decision applying the economic loss doctrine to Petta's negligence claim because: (1) the duty at issue exists purely in tort and does not arise from any agreement between the parties; (2) Petta's claim does not create a risk of limitless litigation and, instead, limits claims to a foreseeable group of people (those specific people whose personal information Christie stored and was breached) who experienced a defined harm (the theft of their personal and medical information); and (3) this case is not one alleging "purely economic losses", but also alleges the impairment of an intangible good (personal and private medical information) due to its theft and misuse

A. The Duties and Injuries at Issue Did Not Arise from a Contract

A principal purpose of the economic loss doctrine in Illinois is to prevent recovery in tort for a breach of a contractual duty. As this Court has explained:

> Contract law serves a vital commercial function by providing sellers and buyers with the ability to define the terms of their agreements with certainty prior to a transaction. Where the duty of a seller has traditionally been defined by contract, therefore, *Moorman* dictates that the theory of recovery should be limited to

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

> contract although recovery in tort would be available under traditional tort theories.

Fireman's Fund Ins. Co. v. SEC Donohue, Inc., 176 Ill. 2d 160, 164(1997) (citing *Congregation of the Passion, Holy Cross Province v. Touche Ross & Co.*, 159 Ill.2d 137, 159–60 (1994)).

Consequently, "the economic loss, or commercial loss, doctrine denies a remedy in tort to a party whose complaint is rooted in disappointed contractual or commercial expectations." *Sienne Ct. Condominium Ass'n v. Champion Aluminum Corp.*, 2018 IL 122022, ¶ 21; *see also Hecktman v. Pac. Indem. Co.*, 2016 IL App (1st) 151459, ¶ 14 ("The rationale behind the *Moorman* doctrine is that . . . contract law and the Uniform Commercial Code (UCC) provide remedies for economic losses from diminished commercial expectations . . . ."); *In re Illinois Bell Switching Station Litig.*, 161 Ill.2d 233, 241 (1994) ("The *Moorman* court concluded that qualitative defects are best handled by contract rather than tort law."). Therefore, "[w]here a duty arises outside of the contract, the economic loss doctrine does not prohibit recover in tort for the negligent breach of that duty." *See Congregation*, 159 Ill. 2d at 162 ("The evolution of the economic loss doctrine shows that the doctrine is applicable . . . only where the duty of the party performing the service is defined by the contract that he executes with his client.").

Here, Petta is not seeking to recover in tort for any losses caused by disappointed contractual or commercial expectations. She is seeking to recover for harm she experienced due to Christie's conduct wholly outside of any

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

agreed-upon medical services that Christie provided to Petta. *See Flores*, 2023 IL App (1st) 230140, ¶ 57 (declining to apply the economic loss doctrine because "plaintiffs' injuries [arose] from defendant's alleged breach of its duty to safeguard personal information incidental to the transaction" and their claims were "based on the common law duty to safeguard personal information rather than any express contractual duty."); *Marriott*, 440 F. Supp. 3d at 475–76 ("[D]ata security breach cases do not fit neatly into the paradigm of the cases that led to the adoption of the economic loss doctrine" because "the injury sustained by the consumer has nothing at all to do with the quality or fitness of the 'product' purchased"); *Dittman*, 649 Pa. at 516 (holding plaintiffs' claims arising out of a data breach were not barred by the economic loss doctrine because the "legal duty [to protect personal information] exists independently from any contractual obligations between the parties[.]").

Indeed, the duty alleged here—that Christie was required to implement reasonable data security measures—does not arise out of any agreement related to the medical services Christie provided. Instead, that duty arises out of statutory law and common law due to the foreseeable harm to Petta should Christie implement poor data security. 815 ILCS 530/45(a); 15 U.S.C. § 45(a)(1). Christie's obligation to reasonably secure patient data, therefore, is not a contractual expectation or requirement but is one that "society recognizes . . . exist[s] wholly apart from any contractual undertaking . . . to protect fellow citizens from unreasonable risks of harm." *Collins v. Reynard*, 154 Ill. 2d 48,

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

51 (1992). Petta's harm is due to Christie's violation of that societal expectation, not an economic loss attributable to disappointed contractual expectations. Those are the exact type of circumstance where tort law, rather than contract law, governs. *Id.* at 1186–87.

B. Data Breach Actions Do Not Pose a Risk of Unbounded Liability

In addition to preventing plaintiffs from using tort law to circumvent contractual duties and remedies, this Court has also stated that the economic loss rule exists to prevent the possibility of "virtually endless" liability where defendants are "held liable for every economic effect of its tortious conduct" and "would face virtually uninsurable risks" that are "far out of proportion to its culpability." *City of Chicago v. Beretta U.S.A. Corp.*, 213 Ill. 2d 351, 418 (2004). That, however, is not a concern in actions arising from a data breach because liability is limited to those specific individuals whose information the defendant collected and stored, failed to protect, and were ultimately impacted by the data breach. *See Toretto v. Donnelley Fin. Sols., Inc.*, 583 F. Supp. 3d 570, 594 (S.D.N.Y. 2022) ("[T]he imposition of a duty does not open [the defendant] up to limitless liability" because the "potential liability is limited to the individuals whose personal information it obtained while providing its services."); *Marriott*, 440 F. Supp. 3d at 476 ("[D]ata security breach cases have very little in common with . . . the policies that underlie [the economic loss] rule", including "protecting manufacturers of defective products from

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

unlimited liability to persons they may have had no direct contract with from tort claims[.]").

Here, Petta and the other victims of the Data Breach are not unknown individuals with downstream injuries attenuated from the initial incident. Rather, Petta has a direct relationship with Christie as its patient. L.R. C197 V2, ¶ 17. As a result of receiving medical services from Christie, it obtained Petta's personal and medical information, which it collected and stored. *Id.* Consequently, Christie knew of Petta, collected and retained her sensitive data, and knew or should have known that a data breach threatened to directly harm her. Petta is, thus, in the very group of individuals foreseeably harmed by Christie's alleged inadequate data security.

Moreover, Petta's injury—the theft and misuse of her personal information—is precisely the type of injury expected from a data breach, and the very risk that has prompted the data security requirements that entities like Christie must satisfy. This type of risk, moreover, is fully insurable, and entities with sensitive data often obtain cybersecurity insurance the covers potential liability arising from a data breach like Christie's, further indicating that the injuries here are not attenuated but rather, expected. *See Beretta*, 213 Ill. 2d at 418 (discussing the need to avoid imposing "virtually uninsurable risks" on negligent actors). Thus, Christie does not face "limitless" liability from its Data Breach—they would be liable only to the specific group of people whose information they collected and stored, and which was breached).

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

C. Christie Impaired the Value, Integrity, and Confidentiality of Petta's Private Information

The Court should not apply the economic loss doctrine here for a final reason: Petta did not allege she suffered "purely economic losses." Under the *Moorman* doctrine, the economic loss doctrine does not apply where the plaintiff suffered an injury to their person or property. *See In re Chicago Flood Litig.*, 176 Ill. 2d 179, 198 (1997) (requiring a plaintiff to have alleged "physical property damage"). The reason for such a requirement is, again, to prevent endless liability because "the economic consequences of any single accident are virtually limitless." *Id.* Requiring physical property damage ensures a close nexus between the plaintiff's injury and the accident, thereby preventing endless liability. *Id.* at 378 (explaining that "the economic loss doctrine avoids the consequences of open-ended tort liability.").

Here, Petta alleges that her personal and medical information derives value from its confidentiality and, by failing to secure it, Christie irreparably harmed the value of that information because it is no longer private but in the hands of cybercriminals. L.R. at C206 V2, ¶¶ 54–63; C221 V2, ¶ 119. Petta here suffered damage to her intangible personal information, which was stolen and actively misused. The impact of the Data Breach on her personal information, a form of intangible property, offers a sufficient nexus between Petta's injuries and the Data Breach to obviate the concern of limitless liability.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Most courts now recognize that a data breach impairs the privacy, confidentiality, and value of the impacted information. "[T]he growing trend across courts that have considered this issue is to recognize the lost property value of information" caused by its theft in a data breach." *Marriott*, 440 F. Supp. 3d at 460–61 (collecting cases); *see also In re Experian Data Breach Litig.*, No. 15-cv-151592, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016) ("[A] growing number of federal courts have now recognized the Loss of Value of [personally identifying information] as a viable damages theory." (internal quotations omitted)); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No 16-md-2752, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (accepting allegations that "[data [b]reaches cause[] all [p]laintiffs to suffer a loss of value of their [personally identifying information.]").

Illinois similarly recognizes that intangible information has value and constitutes property. *See* 720 ILCS 5/15-1 (defining "property" in the context of theft to include "anything of value" including "records, recordings, documents . . . computer programs or ***data*** . . . ." (emphasis added)); 720 ILCS 5/17-55(2)–(3) (prohibiting computer fraud and defining "property" to mean, among other things, "electronically produced data" and "confidential, copyrighted, or proprietary information[.]")). Illinois also recognizes individuals have a property interest in the use of one's identity. *See, e.g.*, *Ainsworth v. Century Supply Co.*, 295 Ill. App. 3d 644, 650 (1998) ("The

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

appropriation of plaintiff's image is more properly in the nature of a usurpation of a plaintiff's property rights in the exclusive use of his image.").

The theft and impairment of Petta's personal information constitutes damage to an intangible good, creating a nexus between Christie's wrongdoing and Petta's harm, overcoming any concerns of limitless liability. As such, the Court should find the economic loss doctrine does not apply.

IV. PETTA SUFFICIENTLY ALLEGED A CLAIM FOR VIOLATION OF PIPA THROUGH THE ICFA

The trial court incorrectly held Petta did not allege a claim for Christie's violation of PIPA. L.R. at C443 V2. Although the Fifth District did not address this issue, the trial court held PIPA does not provide a private cause of action and that Plaintiff did not suffer a sufficient injury to bring such a claim. The Court should reverse the Trial Court's ruling on both grounds.

First, the ICFA affords plaintiffs a cause of action for a violation of PIPA. Under the ICFA, "[a]ny person who suffers actual damage as a result of a violation of [the ICFA] committed by any other person may bring an action against such person." 815 ILCS 505/10a(a). PIPA, furthermore, states that "[a] violation of this Act constitutes an unlawful practice under the [ICFA]." 815 ILCS 530/20. Here, Petta alleged Christie violated PIPA by both failing to implement reasonable data security measures and by failing to reasonably notify Petta of the Data Breach, both of which violate PIPA and, consequently, the ICFA. 815 ILCS 530/10(a); 815 ILCS 530/45(a). Christie's alleged violation of the PIPA is actionable under the ICFA.

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Second, Petta adequately alleged actual damages sufficient to bring a claim under the ICFA. 815 ILCS 505/10a(a); s*ee Burkhart v. Wolf Motors of Naperville, Inc.*, 2016 IL App (2d) 151053, ¶ 22 ("[O]nly a person who suffers actual damages as a result of a violation of the [Consumer Fraud] Act may bring a private action."). "The purpose of awarding damages to a consumer-fraud victim is not to punish the defendant or bestow a windfall upon the plaintiff, but rather to make the plaintiff whole." *Burkhart*, 2016 IL App (2d) 151053, ¶ 22.

Here, Petta alleged two types of actual damages. First, she alleged she suffered from the loss of confidentiality and integrity of her personal information, which diminished its value and usefulness. *See* L.R. at C221 V2, ¶ 119; *See Dewan v. Ford Motor Co.*, 363 Ill. App. 3d 365, 369 (2005) (holding "diminished value" of plaintiff's property "is a compensable injury in consumer fraud[.]"); *Marriott*, 440 F. Supp. 3d at 462. Second, Plaintiff alleged she lost the value of the time and effort she spent mitigating the risk caused by the Data Breach, specifically, the threat of present and future fraud and identity theft. L.R. at C221V2, ¶ 119; *see Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018) (holding that "the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective" and "can justify money damages, just as they support standing.").[10]

[10] Moreover, Petta may still have the availability of nominal damages for a knowing breach of the ICFA. *See Kirkpatrick v. Strosberg*, 385 Ill. App. 3d 119,

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

While Christie has argued Plaintiff's alleged damages are "speculative," that is a fact issue to be resolved by a factfinder, not a basis to dismiss Petta's claim altogether. *See, e.g.*, *Williams v. Manchester*, 228 Ill. 2d 404, 425, 888 N.E.2d 1, 13 (2008) (holding that an "increased risk of harm is an *element of damages* that can be recovered for a present injury[.]") (emphasis in original)). The Court should find Petta, at this stage, adequately alleged Christie's violation of the ICFA.

CONCLUSION

The Court should reverse the Fifth District Appellate Court, find Petta has standing to bring her claims and, additionally, hold that Petta may pursue a negligence claim for Christie's alleged breach of its common law duty and may pursue a claim under the ICFA for Christie's alleged violation of PIPA.

Dated: May 2, 2024

/s/ David M. Cialkowski

David M. Cialkowski, IL No. 6255747
Brian C. Gudmundson
Michael J. Laird
Rachel K. Tack
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
david.cialkowski@zimmreed.com
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

894 N.E.2d 781 (2008) (permitting nominal damages where plaintiff proved they suffered actual damages but could not adequately calculate the amount).

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

Christopher Jennings
JENNING PLLC
P.O. Box 25972
Little Rock, AR 72221
Telephone: (501) 247-6267
chris@jenningspllc.com

Attorneys for Plaintiff-Appellant Rebecca Petta

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 49 pages or 12,932 words.

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

Dated: May 2, 2024

/s/ David M. Cialkowski
David M. Cialkowski

Attorney for Plaintiffs-Appellants'

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

CERTIFICATE OF SERVICE

I hereby certify that on May 2, 2024, I electronically filed Plaintiffs-Appellants' Brief and Appendix with the Clerk of the Supreme Court of Illinois using an approved Electronic Filing Service Provider ("EFSP"). I further certify that a copy of the same was served via electronic mail upon the following:

Jonathan B. Amarilio
Jeffrey M. Schieber
Jaimin H. Shah
Taft Stettinius & Hollister LLP
111 E. Wacker Drive, Suite 2600
Chicago, IL 60601
jamarilio@taftlaw.com
jschieber@taftlaw.com
jshah@taftlaw.com

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

Dated: May 2, 2024

/s/ David M. Cialkowski
David M. Cialkowski

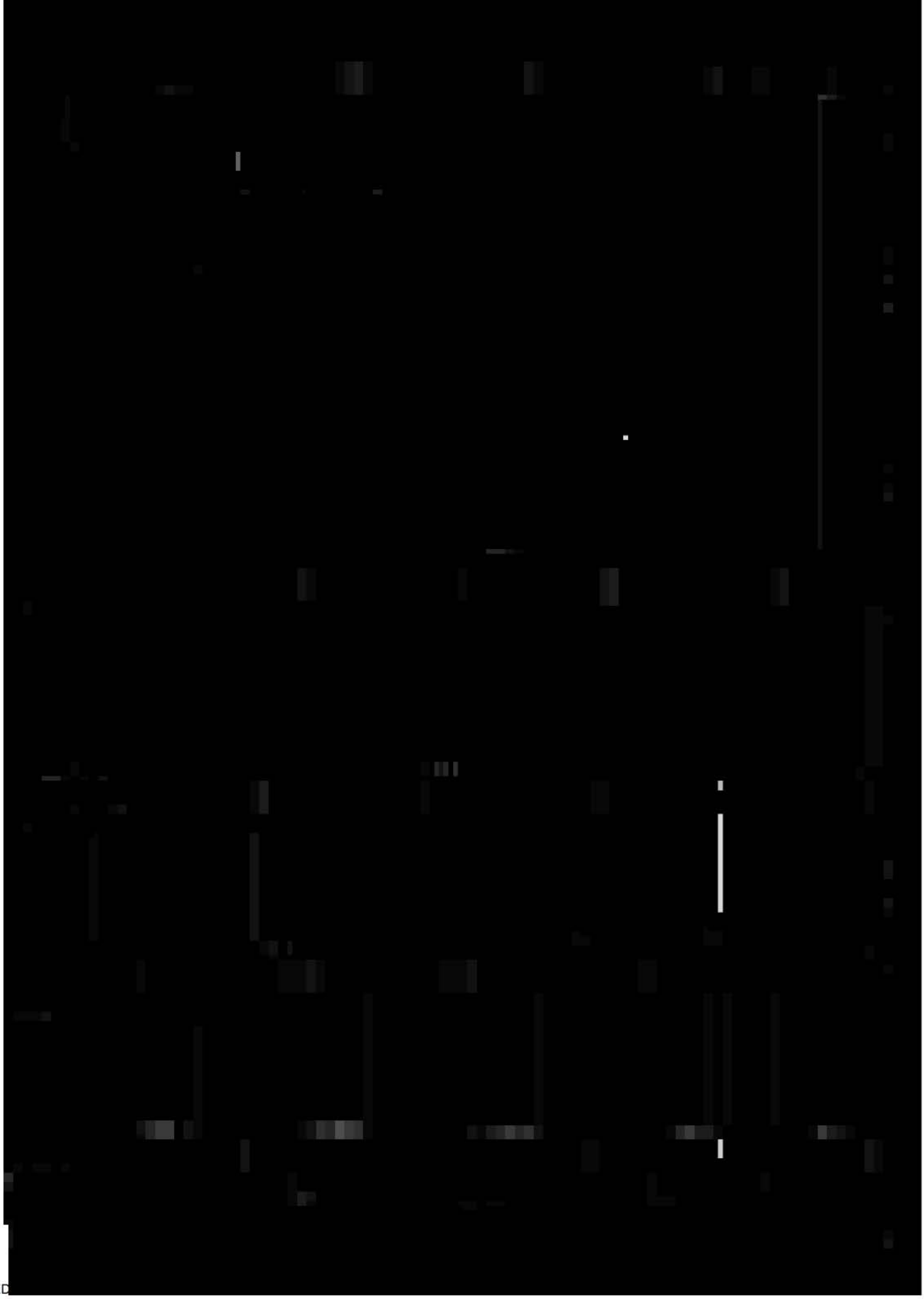
Attorney for Plaintiffs-Appellants'

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

INDEX TO APPENDIX

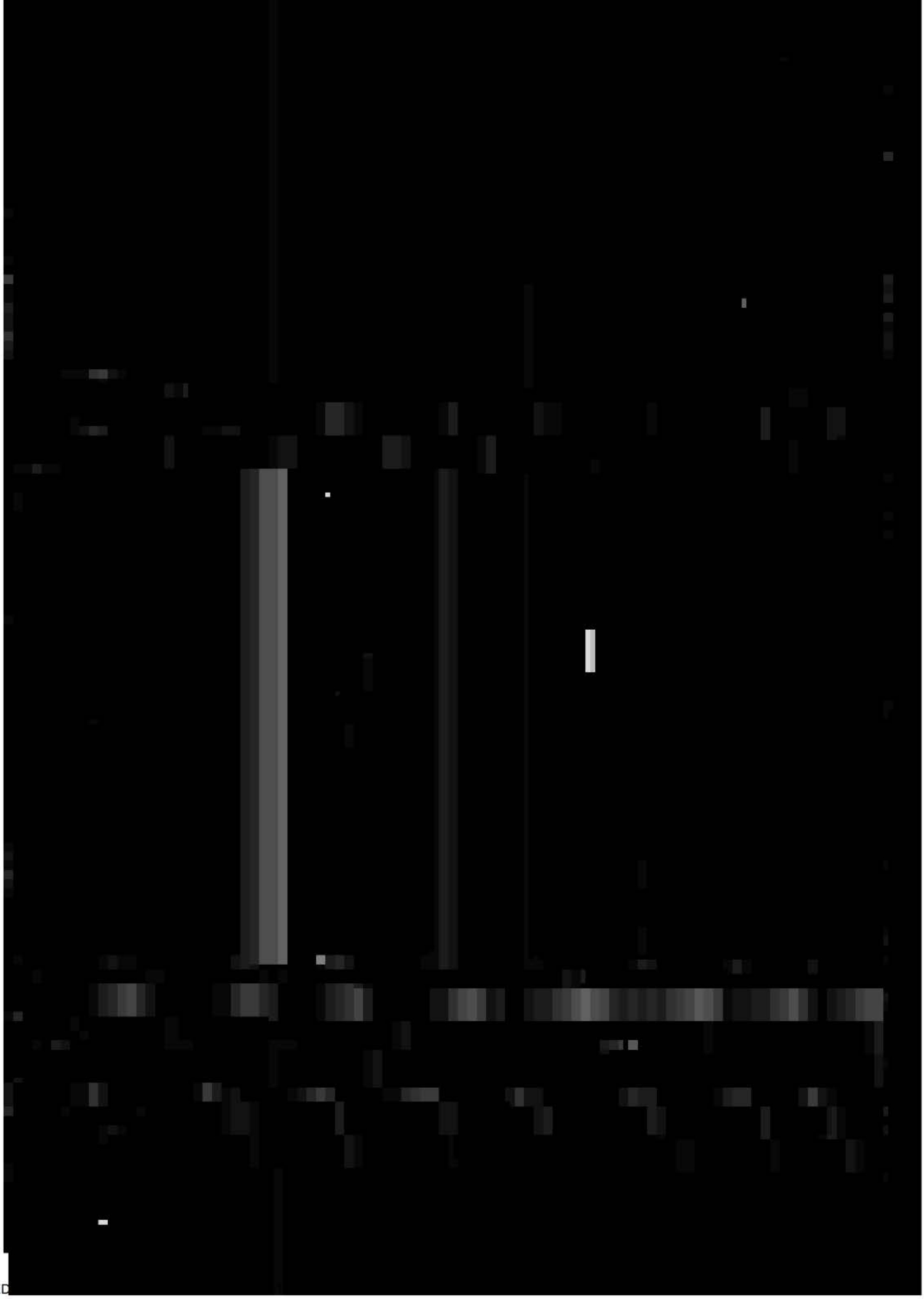
SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

A001

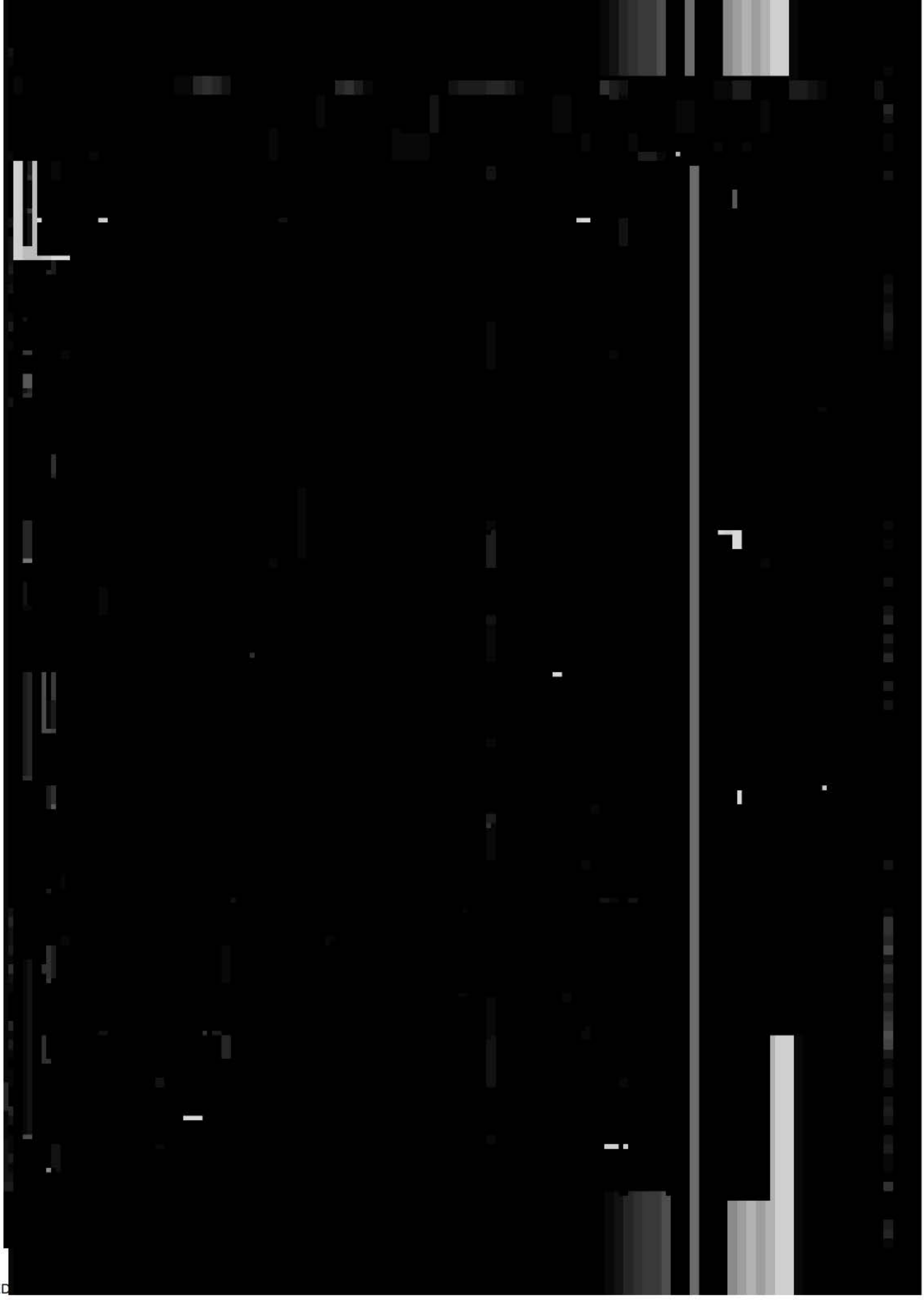


SUBMITTED

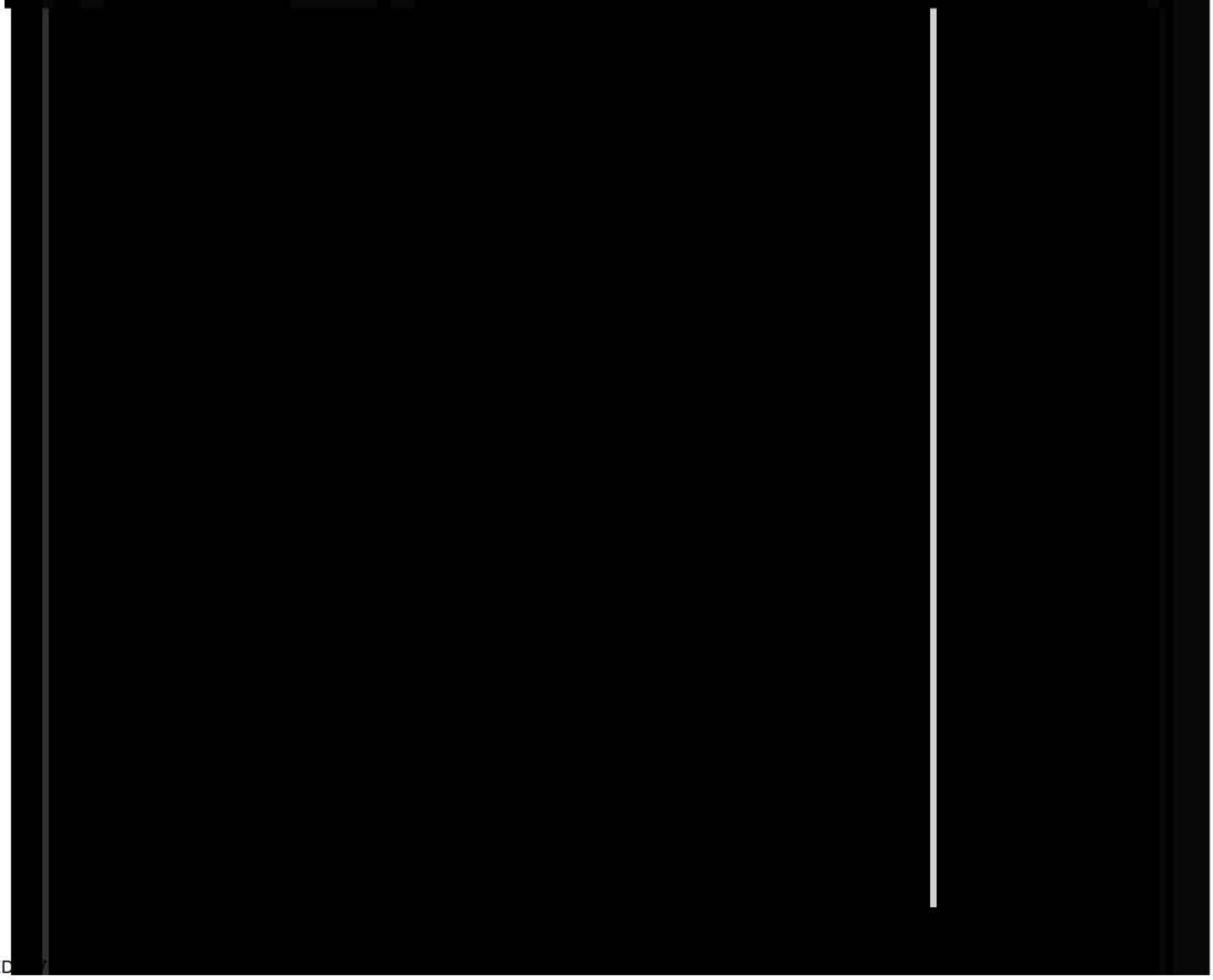
SUBMITTED



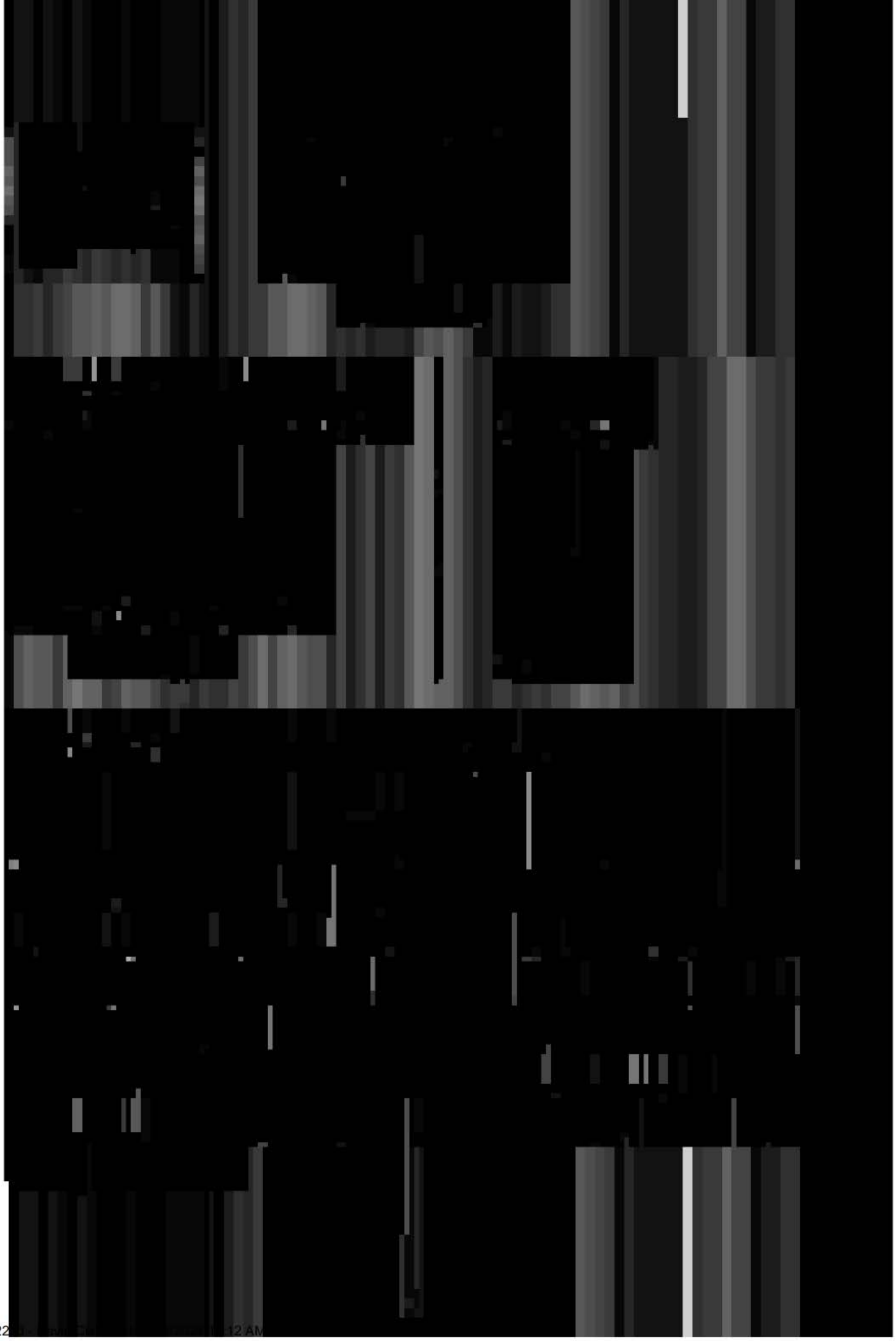
SUBMITTED



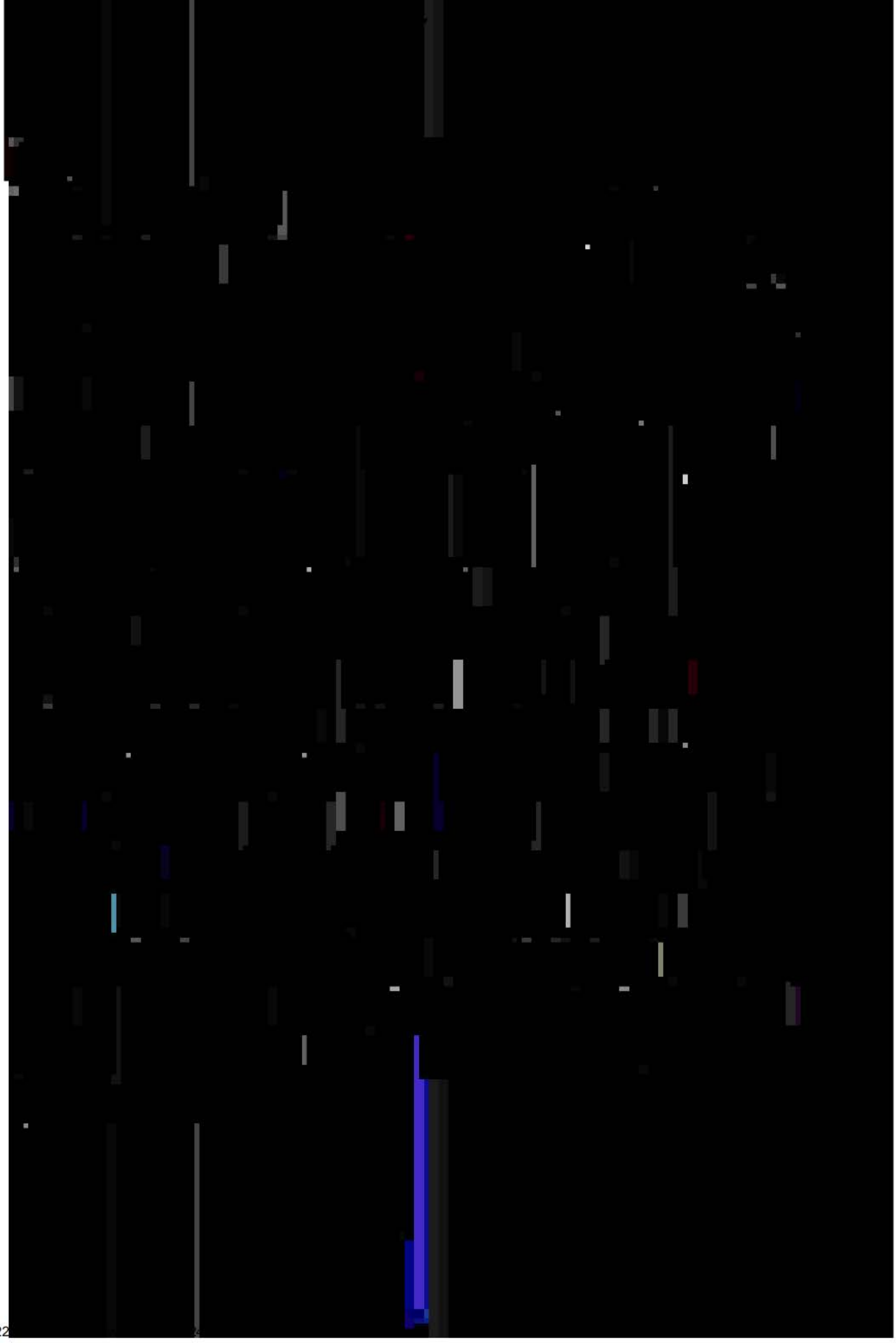
SUBMITTED



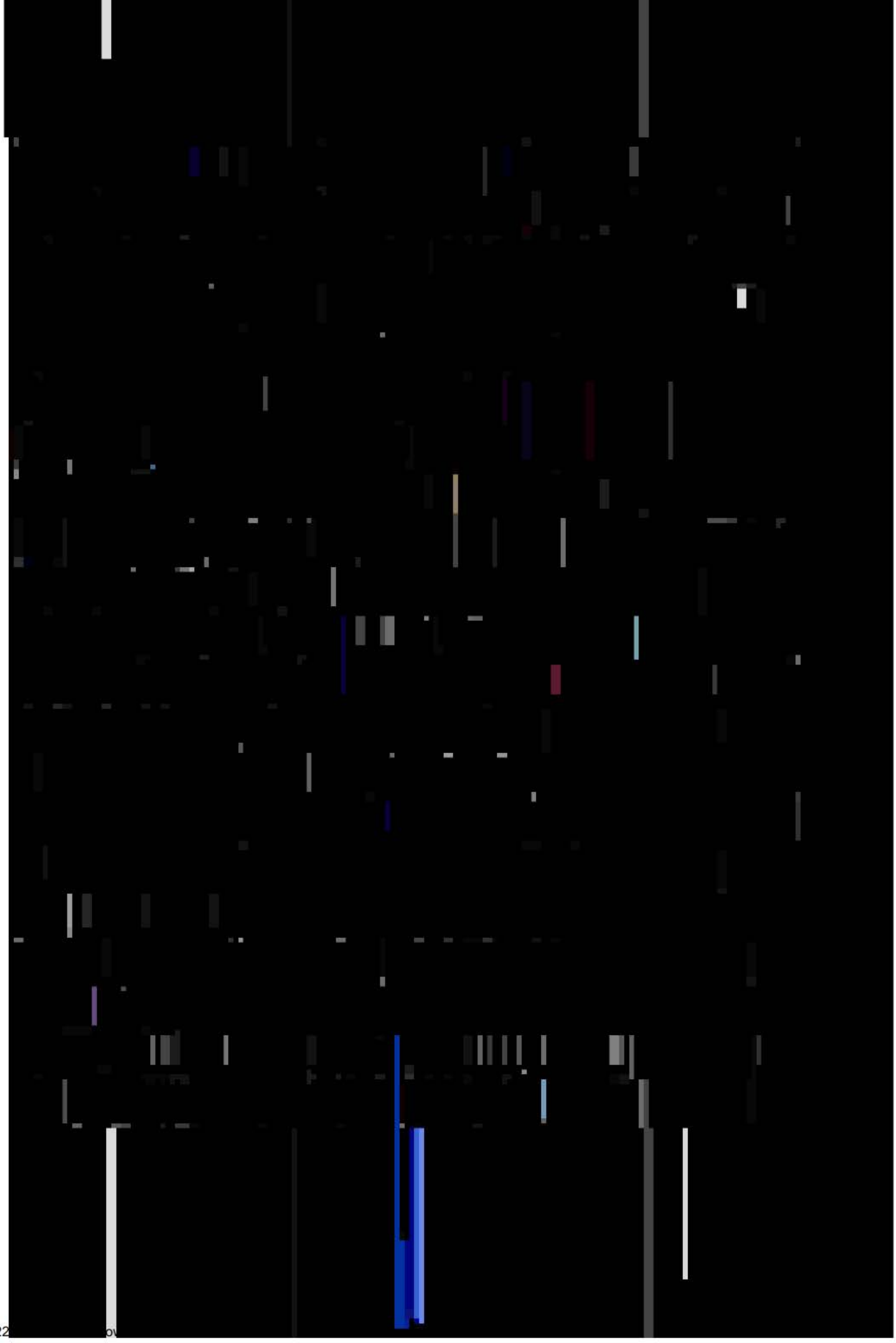
SUBMITTED



SUBMITTED - 275322

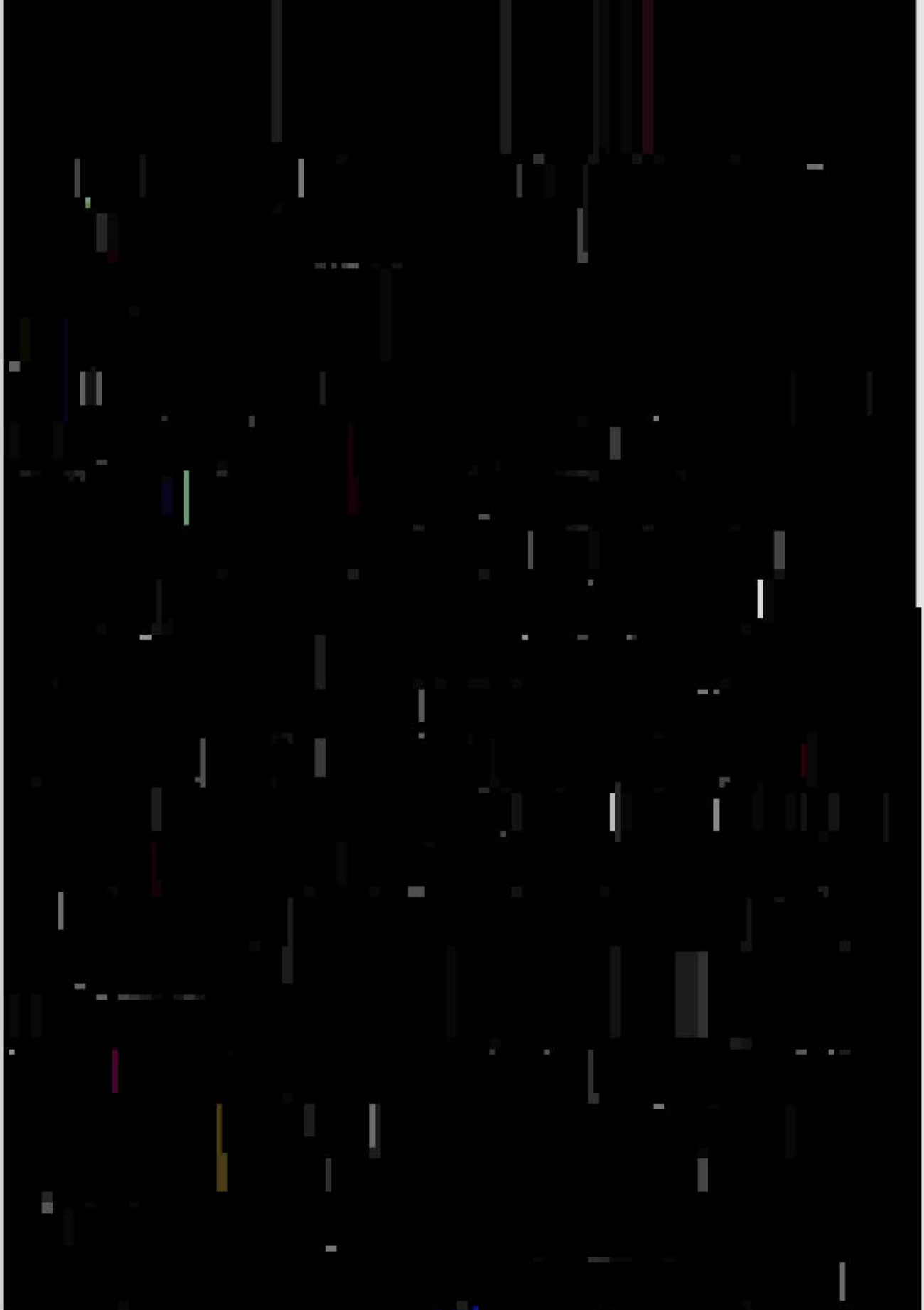


SUBMITTED - 275322



SUBMITTED - 275322

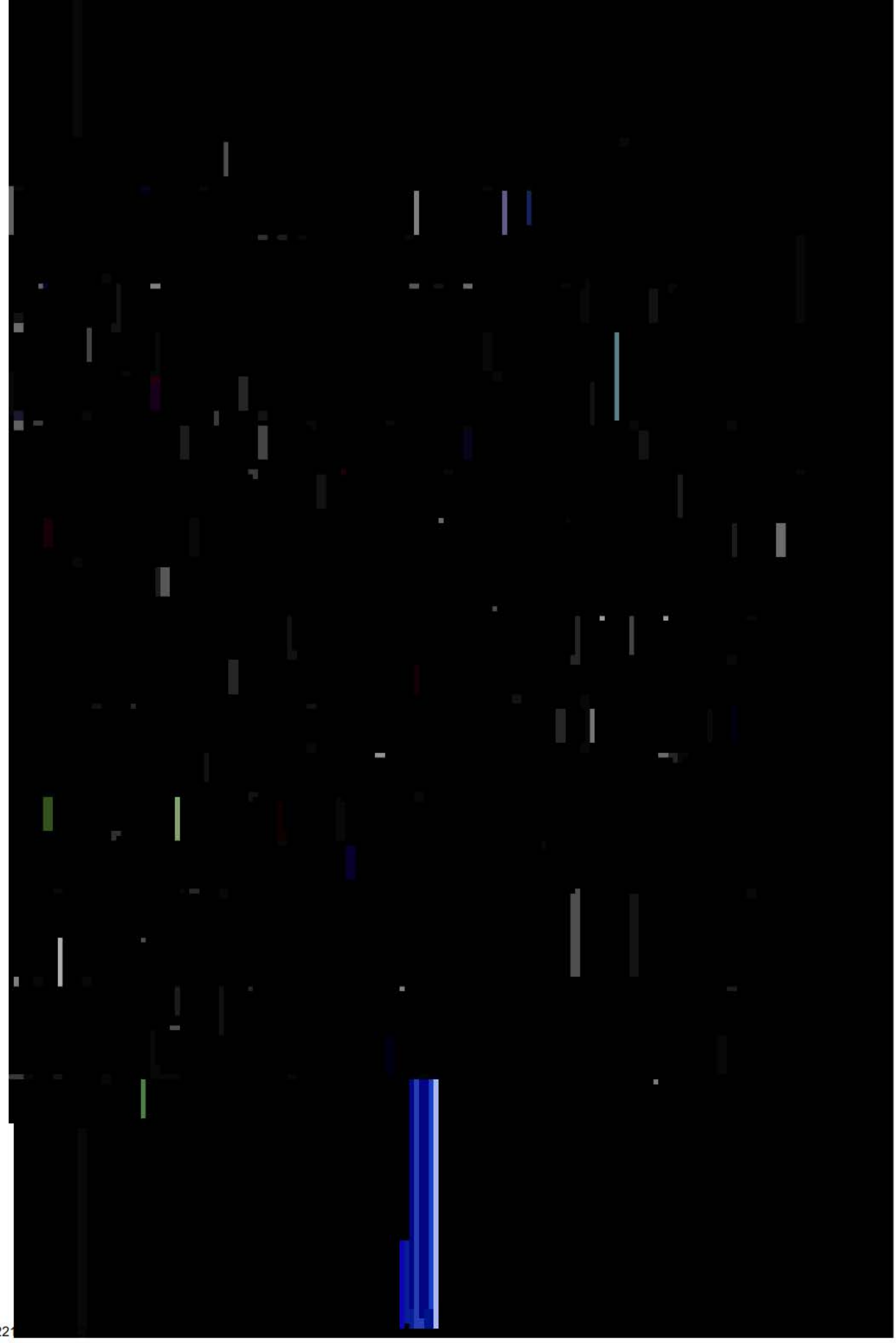
SUBMITTED - 275322



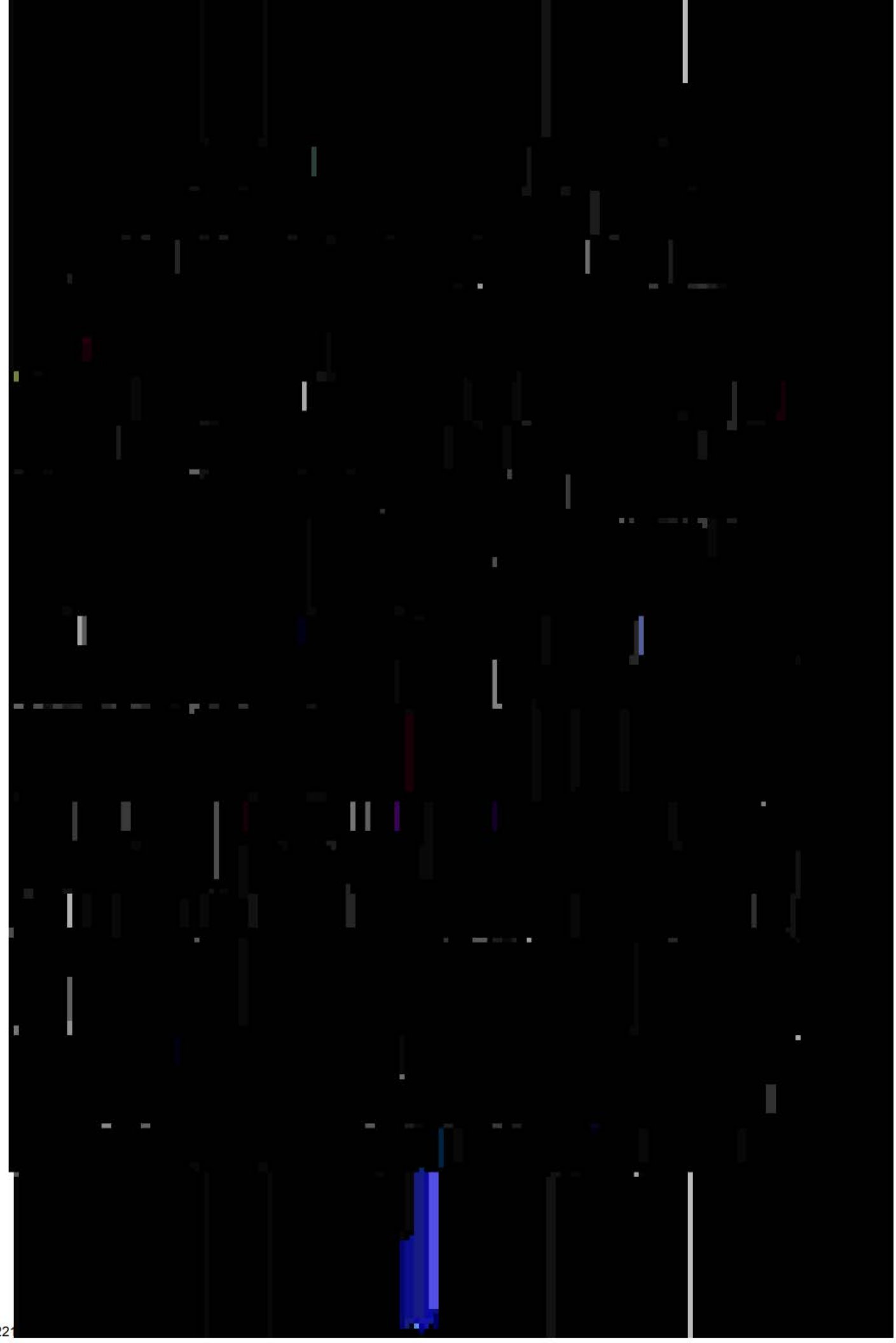
SUBMITTED - 2753221

SUBMITTED - 275322

SUBMITTED - 2753221

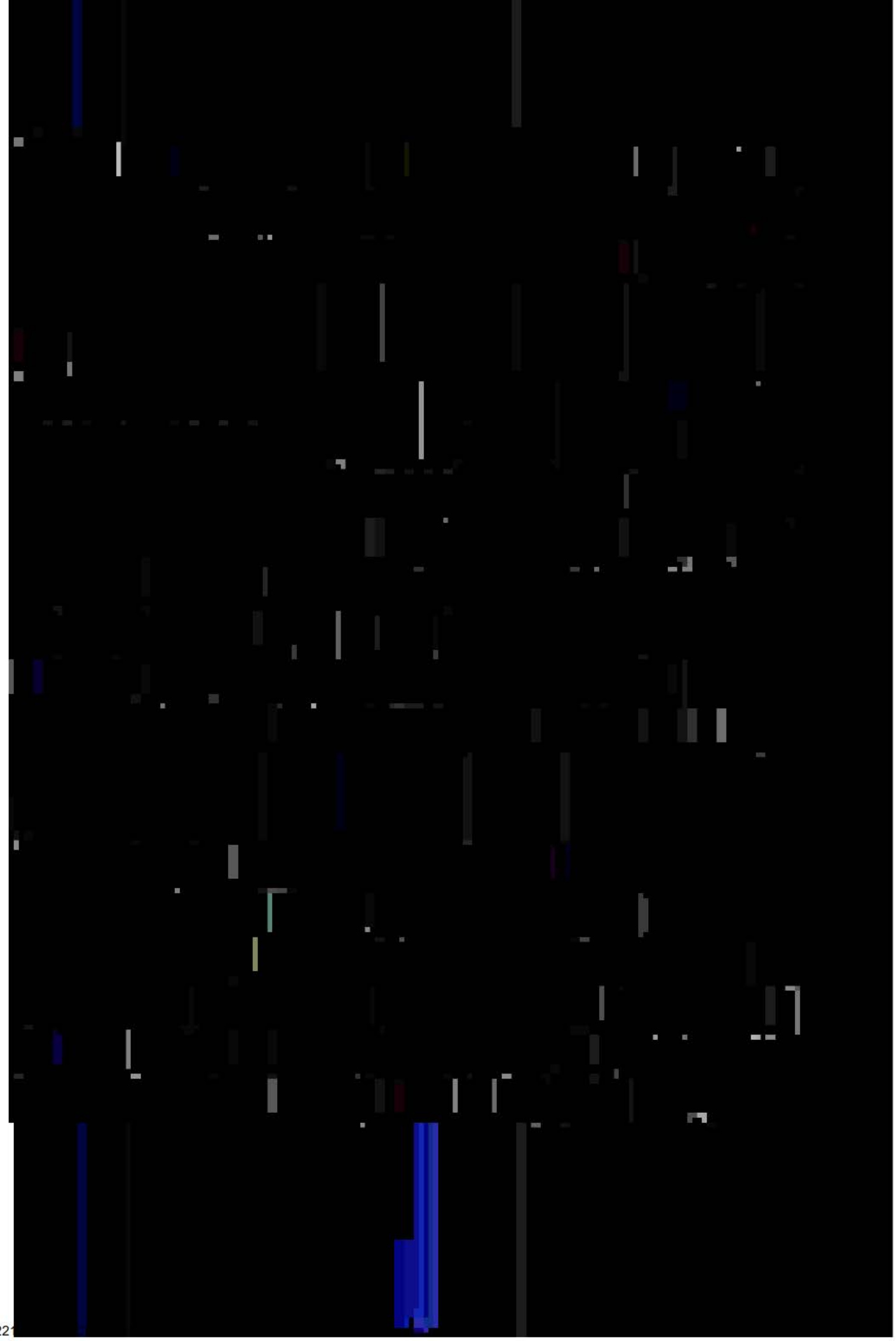


SUBMITTED - 2753221

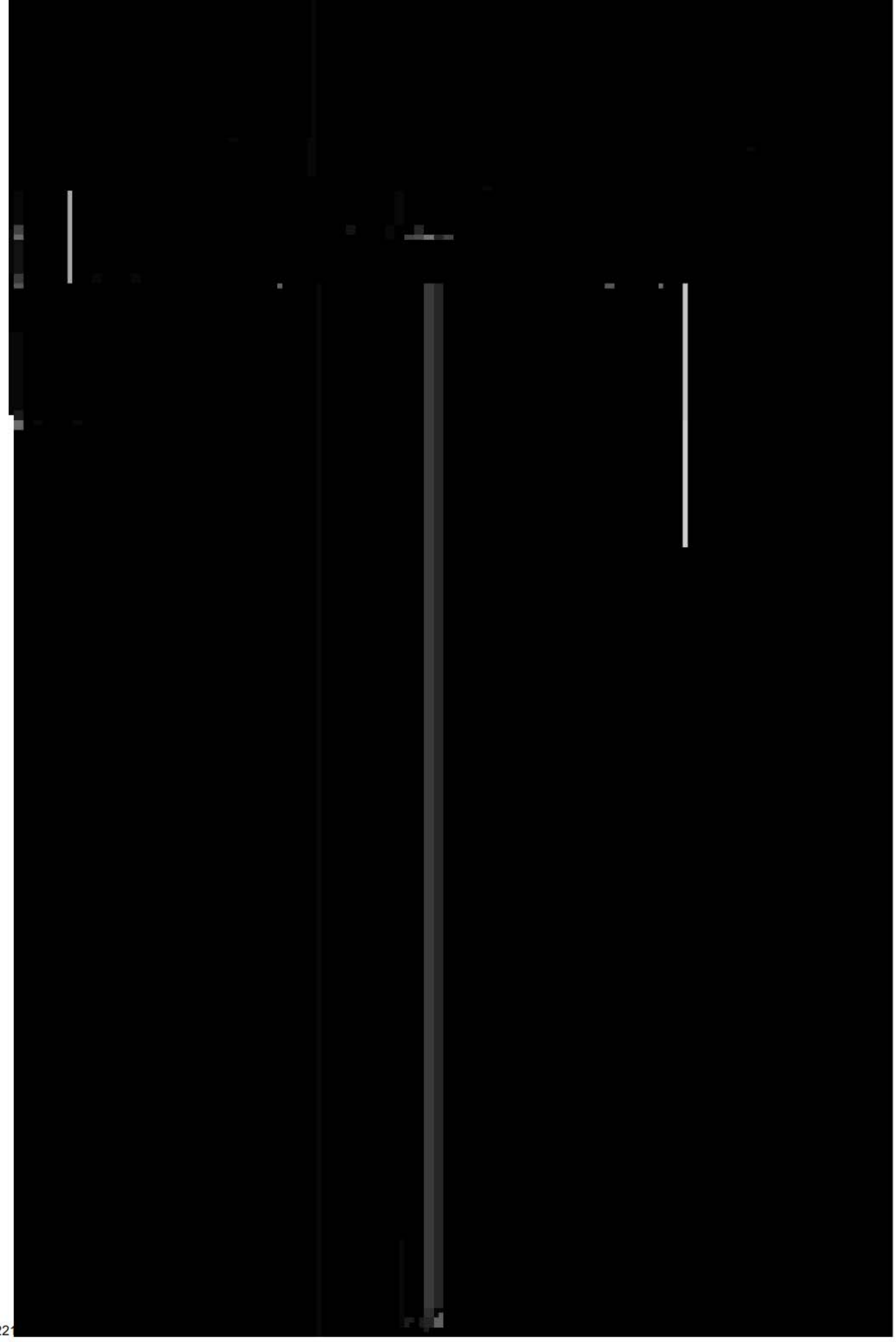


SUBMITTED - 2753221

SUBMITTED - 275322



SUBMITTED - 2753221



SUBMITTED - 2753221

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11

APPEAL TO THE APPELLATE COURT OF ILLINOIS
FIFTH JUDICIAL DISTRICT
FROM THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
CHAMPAIGN COUNTY, ILLINOIS

Rebecca Petta, on her own behalf, and behalf of those similarly situated, Petitioner,	)	APPELLATE CASE:5-22-0742
— vs —	)	CIRCUIT CASE:22-LA-51
Christie Business Holdings, P.C. (d/b/a Christie Clinic), Respondent.	)	TRIAL JUDGE: Bohm

COMMON LAW RECORD – TABLE OF CONTENTS

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

APPEAL TO THE APPELLATE COURT OF ILLINOIS
FIFTH JUDICIAL DISTRICT
FROM THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
CHAMPAIGN COUNTY, ILLINOIS

Rebecca Petta, on her own behalf, and behalf of those similarly situated, Petitioner,	)	
— vs —	)	APPELLATE CASE:5-22-0742
	)	CIRCUIT CASE:22-LA-51
	)	TRIAL JUDGE: Bohm
Christie Business Holdings, P.C. (d/b/a Christie Clinic), Respondent.	)	

Date Filed	Title/Description	Page No.
8/23/2022	Appearance Verified Statement of Out-of-State Attorney Pursuant to	C402-C404 V2
8/23/2022	Appearance Verified Statement of Out-of-State Attorney Pursuant to	C405 V2
9/1/2022	Verified Statement Of Out-Of-State Attorney Pursuant To Supreme	C406-C411 V2
10/26/2022	Letters Letter from Brian Gudmundson to Judge Bohm Submitting	C412 V2
10/26/2022	Letters Letter from Brian Gudmundson to Judge Bohm Submitting	C413-C428 V2
10/28/2022	Order on Motion to Dismiss	C429-C441 V2
11/16/2022	Notice of Appeal	C442-C443 V2
11/17/2022	Appellate Court's letter to counsel pursuant to	C444 V2
11/30/2022	PLAINTIFF DOE'S NOTICE OF APPEAL	C445-C460 V2
12/1/2022	Appellate Court Docketing Order on File.	C461 V2
12/2/2022	Appellate Court's letter to counsel pursuant to	C462-C463 V2

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM

APPEAL TO THE APPELLATE COURT OF ILLINOIS
FIFTH JUDICIAL DISTRICT
FROM THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
CHAMPAIGN COUNTY, ILLINOIS

Rebecca Petta, on her own behalf, and hehalf of those similarly situated
Plaintiff/Petitioner

Appellate Court No: 5-22-0742
Circuit Court No: 22-LA-51
Trial Judge: Bohm

v.

Christie Business Holdings, P.C.
(d/b/a Christie Clinic)
Defendant/Respondent

E-FILED
Transaction ID: 5-22-0742
File Date: 1/11/2023 3:18 PM
John J. Flood, Clerk of the Court
APPELLATE COURT 5TH DISTRICT

REPORT OF PROCEEDINGS – TABLE OF CONTENTS

Page 1 of 1

SUBMITTED - 27532213 - David Cialkowski - 5/6/2024 11:12 AM