

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CHRISTINE McGOVERAN, JOSEPH
VALENTINE, and AMELIA RODRI-
GUEZ, on behalf of themselves and all
other persons similarly situated, known
and unknown,

Plaintiffs,

No. 1:20-cv-01399-SB

v.

AMAZON WEB SERVICES, INC. and
PINDROP SECURITY, INC.,

Defendants.

Alexander L. Braitberg, Joshua A. Katz, Andrew D. Schlichter, Joel Rohlf,
SCHLICHTER BOGARD & DENTON, LLP, St. Louis, MO; Stephen B. Brauerman,
Ronald P. Golden, III, BAYARD, P.A., Wilmington, DE.

Counsel for Plaintiff.

Jody Barillare, MORGAN LEWIS & BOCKIUS LLP, Wilmington, DE; Elizabeth
Herrington, MORGAN LEWIS & BOCKIUS LLP, Chicago, IL; Raechel K. Kummer,
MORGAN LEWIS & BOCKIUS LLP, Washington, DC.

Counsel for Defendant Amazon Web Services, Inc.

Andrew Bloomer, KIRKLAND & ELLIS, Chicago, IL; Diana M. Torres, KIRKLAND &
ELLIS, Los Angeles, CA; Jack B. Blumenfeld, Megan Elizabeth Dellinger, MORRIS,
NICHOLS, ARSHT & TUNNELL LLP, Wilmington, DE.

Counsel for Defendant Pindrop Security, Inc.

MEMORANDUM OPINION

March 29, 2023

BIBAS, *Circuit Judge*, sitting by designation.

Legislation requires tradeoffs. Regulate an industry too strictly, and you could stifle innovation. Take a hands-off approach, and people might be harmed.

Illinois's law regulating the use of biometrics to identify customers reflects these tradeoffs. It limits collecting, retaining, and using consumer biometric data. But it exempts some industries from its rules.

Plaintiffs, all residents of Illinois, have sued defendants for violating Illinois law. Defendants now move to dismiss, arguing that the law does not apply to them and that plaintiffs' allegations fall short. Because they are mostly right, I grant their motions in part.

I. FACTS

A. Illinois's Biometric Information Privacy Act

In 2008, Illinois enacted the Biometric Information Privacy Act. *See* 740 Ill. Comp. Stat. 14/1–14/25. Designed to address “[t]he use of biometrics” in “financial transactions and security screenings,” the Act “regulat[es] the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information” in Illinois. 14/5(a), (g). And it has teeth: “[a]ny person aggrieved by a violation” of the Act can sue for liquidated damages. *Id.* 14/20 (awarding \$1,000 for negligent violations and \$5,000 for intentional or reckless violations). Plaintiffs can also recover attorneys’ fees and costs. *Id.*

The Act regulates the use of both “biometric identifiers” and “biometric information.” *See* 14/15. Rather than generally defining “biometric identifiers,” the Act simply lists the six things that count: “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 14/10. On the other hand, the Act defines “biometric information” generally: “any information ... based on an individual’s biometric identifier used to identify an individual.” *Id.* The Act had to define and regulate biometric information, not just identifiers, to ensure that companies did not convert identifiers into numbers or some other format—thus creating information not on the Act’s list of identifiers—and then use that information to identify people. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1095, 1097 (N.D. Ill. 2017).

The parties sometimes use “biometric identifiers” and “biometric information” interchangeably. But as we will see, the distinction can make a difference. For clarity, I will use “biometric data,” a term that the Act does not use, when I refer to both.

B. Plaintiffs’ suit

At the motion-to-dismiss stage, I take all well pleaded allegations in plaintiffs’ Amended Complaint as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

Plaintiffs all live in Illinois and are customers of John Hancock, a financial-services company that offers retirement products. Am. Compl., D.I. 47 ¶¶ 6–8, 98–101. At various times in 2019, they called John Hancock to discuss their retirement accounts. ¶¶ 98–101. John Hancock used Amazon Connect, a product offered by defendant Amazon Web Services, to receive and process those calls. ¶¶ 51, 98, 102.

Amazon Connect provides cloud-based call centers. ¶¶ 50–55. People dial phone numbers to reach companies like John Hancock, and Amazon servers receive those

phone calls, process voice commands, and connect callers to live agents. ¶¶ 50–55, 121, 123. Amazon also offers voice authentication, an add-on service that confirms callers’ identities using their voiceprints without requiring them to enter a PIN. ¶¶ 37–39, 64–69, 80, 103, 140.

Amazon authenticates callers by using defendant Pindrop’s technology. ¶¶ 64–68, 102–05. Pindrop is a tech company offering “biometric voice products and services.” ¶¶ 57–63. Its technology can process live audio from callers, identify their unique voiceprints, and confirm whether they are who they claim to be. *Id.*; *see also* ¶ 77. Amazon uses Pindrop’s technology as a software plugin. ¶ 69. People call in to an Amazon call center, Amazon routes the call audio to Pindrop’s servers, and Pindrop extracts the callers’ unique biometric data to authenticate them. ¶¶ 78–80. This all seamlessly happens in real time during the phone call. ¶¶ 67, 71, 73, 77.

At various points in the Complaint, plaintiffs allege both that Pindrop itself authenticates callers and that Amazon authenticates callers using biometric data that Pindrop has extracted and then sent to Amazon. *Compare* ¶¶ 59–61, 103, *with* ¶¶ 78, 80, 86, 88. And recently, Amazon developed its own technology to process voiceprints and authenticate callers without Pindrop. ¶ 69. In any event, Amazon and Pindrop both used their technology to authenticate plaintiffs when they called John Hancock. ¶¶ 98, 102–03.

Believing that defendants’ use of their voiceprints violated the Act, plaintiffs filed this suit in Illinois state court as a class action. D.I. 34, at 4. Defendants then removed to federal court and had the case dismissed for lack of personal jurisdiction. *Id.* So

plaintiffs refiled here in the District of Delaware, where both defendants are incorporated. D.I. 1 ¶¶ 10, 12. The Court then dismissed because the Act does not apply outside of Illinois, and plaintiffs had not alleged that defendants had acted in Illinois. D.I. 34, at 12.

Plaintiffs have now filed their First Amended Complaint, which makes several allegations about defendants' activities in Illinois. *See, e.g.*, D.I. 47 ¶¶ 108–34. Their claims come in four counts, each corresponding to a subsection of the Act's overall duty section. ¶¶ 178–207 (citing 740 Ill. Comp. Stat. 14/15(a)–(d)). And they ask me to enjoin defendants from further violating the Act. D.I. 47, at 40 (citing 14/20(4)).

Both Pindrop and Amazon now move to dismiss on several grounds. I must decide if plaintiffs have alleged “sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Iqbal*, 556 U.S. at 678 (internal quotation marks omitted).

II. I DISMISS ALL CLAIMS AGAINST PINDROP

A. Plaintiffs lack standing to bring Count I, Count III, or a claim for injunctive relief against Pindrop

Pindrop says that plaintiffs lack standing to bring some of their claims. Because standing is jurisdictional, I address this argument first. *See N.J. Bankers Ass'n v. Att'y Gen. N.J.*, 49 F.4th 849, 855 (3d Cir. 2022). Pindrop is right: the Complaint fails to show that plaintiffs have standing to bring Count I, Count III, or a claim for injunctive relief.

To have standing, plaintiffs “must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant[s], and (3) that is likely to

be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). To meet the first requirement, they must allege that they have suffered a “concrete—that is, real, and not abstract” injury that has a “close historical or common-law analogue” “traditionally recognized as providing a basis for a lawsuit in American courts.” *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) (internal quotation marks omitted). And to get injunctive relief, they must allege that their injury is “actual or imminent,” that is, “*certainly impending*.” *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 409 (2013) (internal quotation marks omitted).

1. *Count I*. Count I claims that Pindrop violated section 15(a) of the Act. D.I. 47 ¶¶ 178–184. That section requires companies that have biometric data to “develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.” 14/15(a). The written policy must mandate destruction of the biometric data “when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the [company], whichever occurs first.” *Id.* And companies “must comply” with their retention policies. *Id.*

The Seventh Circuit, which encompasses Illinois, has discussed Article III standing for section 15(a) claims. When plaintiffs allege only that a company has failed to develop a written policy, they fail to allege a concrete injury in fact. *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020), *as amended*, 2020 WL 6534581, at *1 (7th Cir. June 30, 2020). The statutory duty to develop and make

available a written policy “is owed to the public generally, not to particular persons whose biometric information the entity collects.” *Id.* So failing to follow section 15(a)’s written-policy requirement does not injure individual plaintiffs in “a concrete and particularized” way. *Id.*

On the other hand, the Seventh Circuit has held that when plaintiffs allege that a company retained their biometric data for longer than section 15(a) permits, they have standing. *See Fox v. Dakota Integrated Sys., LLC*, 980 F.3d 1146, 1154–55 (7th Cir. 2020). It likened retaining data for too long to “an invasion of a private domain, much like an act of trespass” or “a tortious invasion of privacy.” *Id.* at 1154–55 (internal quotation marks omitted). But *Fox* was decided before *TransUnion*. And after *TransUnion*, it is unclear that simply retaining plaintiffs’ biometric data for too long creates standing. *See TransUnion*, 141 S. Ct. at 2209–13 (no standing for claim that defendant maintained inaccurate internal credit reports).

It seems that no case has evaluated *TransUnion*’s effect on *Fox*. But that is a question for another day: plaintiffs have not alleged that Pindrop kept their biometric data past section 15(a)’s deadlines. *See* D.I. 47 ¶¶ 95, 180. They say that they called John Hancock in 2019, and that Pindrop collected their voiceprints then. ¶¶ 98–107. But they do not allege that they are no longer customers of John Hancock, or that Pindrop thus no longer needs their biometric data. Nor do they allege that 2019 was the last time they interacted with John Hancock. So the only section 15(a) violation plaintiffs have alleged is that Pindrop failed to develop a written data-retention policy. *See* ¶¶ 94, 154, 180. That is not enough for standing. *See Bryant*, 958 F.3d at 626.

Plaintiffs point out that they have alleged Pindrop shared their voiceprints with Amazon. D.I. 55, at 9–10. And because their voiceprints were shared, Pindrop could not ensure that the data was retained or destroyed in compliance with section 15(a). *Id.* But the text is clear: section 15(a) requires Pindrop to destroy data in *its possession*. It does not impose a duty on Pindrop to destroy data in *Amazon's* possession. So whatever Amazon might do with data in its possession cannot confer standing on plaintiffs for their claim against Pindrop. This is not a loophole: section 15(d) addresses Pindrop's duty not to “disclose ... or disseminate” (so, share) plaintiffs' biometric data. Plaintiffs have also brought a claim for a section 15(d) violation in Count IV, and Pindrop does not contest plaintiffs' standing there. *See* D.I. 47 ¶¶ 202–07.

2. *Count III.* Plaintiffs allege that Pindrop violated section 15(c), which says that companies may not “sell, lease, trade, or otherwise profit from” someone's biometric data. 740 Ill. Comp. Stat. 14/15(c).

The Seventh Circuit has again provided helpful guidance on standing here. *See Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1246–47 (7th Cir. 2021). In *Thornley*, the Seventh Circuit noted that section 15(c) imposes “a general rule” that companies may not buy and sell biometric data. *Id.* at 1247. So when plaintiffs allege only that a company has broken that rule, but do not allege any “particularized injury resulting from the commercial transaction,” they lack standing. *Id.* But if, for instance, a plaintiff additionally alleges that “the act of selling her data” “deprived her of the opportunity to profit from her biometric information” or “amplified the invasion of her

privacy ... by disseminating it to some unspecified number of other people,” that would support standing. *Id.*

Plaintiffs’ allegations fall short here too. They have not alleged that when Pindrop shared their voiceprints with Amazon, it frustrated their chance to profit from their personal data. They do argue that Pindrop’s sharing their voiceprints amplified their invasion of privacy. D.I. 55, at 10–11. But there was no amplifying. According to the Complaint, Amazon already had access to their call audio and could use its own technology to extract voiceprints from the calls. D.I. 47 ¶¶ 69, 78–80, 86–90. And transferring voiceprints from Pindrop’s servers to Amazon’s is not the sort of public dissemination “to some unspecified number of other people” that counts as an injury in fact. *Thornley*, 984 F.3d at 1246–47; *cf. In re Clearview AI, Inc., Consumer Priv. Litig.*, 2022 WL 252702, at *1, *3 (N.D. Ill. Jan. 27, 2022) (finding a concrete injury when defendants bought access to an online searchable database of face geometries that had been created with “billions of photographs of facial images” that had been “covertly scraped ... from the internet”).

3. *Injunctive relief.* Plaintiffs also lack standing to get an injunction. *See* D.I. 47, at 40. To have standing, they must show that they have an injury that is ongoing, or is at least “imminent,” that is, “*certainly impending.*” *Clapper*, 568 U.S. at 409 (internal quotation marks omitted). And even if Pindrop violated the Act at some point, “past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief ... if unaccompanied by any continuing, present adverse

effects.” *City of Los Angeles v. Lyons*, 461 U.S. 95, 102, 105–07 (1983) (alterations adopted, internal quotation marks omitted).

As Pindrop points out, plaintiffs have not plausibly alleged continuing or imminent harm. D.I. 53, at 15. They do not allege that John Hancock still uses Amazon’s services with Pindrop’s plug-in. Indeed, they allege that Amazon Connect can now function without Pindrop, and that Amazon is working with its partners to ensure compliance with the Act. D.I. 47 ¶¶ 69–70.

Plaintiffs point out that their prayer for injunctive relief is a request for a remedy and not a cause of action. D.I. 55, at 11–12. True, but they still “must demonstrate standing separately for each form of relief sought.” *Friends of the Earth, Inc. v. Laidlaw Env’t Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000) (citing *Lyons*). Plaintiffs also argue that injunctive relief should be available to them because the common-law tort analogues to successful claims under the Act can themselves warrant injunctive relief. D.I. 55, at 12–13. That is also true, but it tells us nothing about plaintiffs’ standing to get injunctive relief here. Without alleging any continuing or imminent violations, they lack standing.

B. The Act’s financial-institution exception applies to Pindrop

Pindrop says that regardless of standing, all claims against it should be dismissed because it is a “financial institution” and thus exempt under the Act. It is right.

1. *Pindrop has not waived this argument.* As an initial matter, plaintiffs say Pindrop waived this argument. D.I. 55, at 5–6 (citing Fed. R. Civ. P. 12(g)(2)). But Pindrop raised the Act’s financial-institution exception in each of its prior motions to dismiss. See D.I. 13, at 18–19; Mot. to Dismiss 15–16, *McGoveran v. Amazon Web*

Servs., Inc., 488 F. Supp. 3d 714 (S.D. Ill. 2020) (No. 3:20-cv-00031-NJR), ECF No. 35. Plaintiffs are right that Pindrop’s arguments have changed: rather than arguing that it qualifies for the exception due to its relationship with John Hancock, it now argues that it qualifies for the exception on its own. *Compare* D.I. 13, at 18–19, *with* D.I. 53, at 4–10. But the bar on successive motions applies to only a “defense or objection” that was previously “omitted.” Fed. R. Civ. P. 12(g)(2). I doubt that this bar applies here: If the financial-institution exception is a defense or an objection, Pindrop has never omitted it. And if Pindrop’s new tack is simply a new argument, then Rule 12(g)(2) does not apply.

Regardless, Pindrop could still raise this argument in its answer, in a judgment on the pleadings, at summary judgment, or at trial. Fed. R. Civ. P. 12(h)(2), 56(a). And Pindrop has not changed its argument to cause needless delay. *See* D.I. 59, at 6 n.10. Plus, plaintiffs have had adequate notice and an opportunity to respond to Pindrop’s argument. D.I. 55, at 5–9. So waiting to address this argument would serve no purpose, and I will consider it now. *Cf.* 5C Charles Alan Wright, Arthur R. Miller & A. Benjamin Spencer, *Federal Practice and Procedure* §1385 (3d ed. 2022).

2. *The Act borrows Gramm-Leach’s definition of “financial institution.”* The Act exempts any “financial institution ... subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 [and its associated regulations].” 740 Ill. Comp. Stat. 14/25(c). (The Act’s text does not explain why the Illinois legislature exempted these institutions. But the legislature may have thought that because Gramm-Leach already subjects financial institutions to comprehensive privacy protections, further regulation was

unnecessary. *See Bryant v. Compass Grp. USA, Inc.*, 503 F. Supp. 3d 597, 601 (N.D. Ill. 2020).) So if Pindrop is a “financial institution,” the Act does not apply.

Pindrop is a tech company, not a “financial institution” in the ordinary sense of the term. But, as we will soon see, Gramm-Leach governs more than just ordinary financial institutions.

One could plausibly read section 25(c)’s exception to apply only to traditional “financial institutions.” *Cf. Patterson v. Respondus, Inc.*, 593 F. Supp. 3d 783, 818–19 (N.D. Ill. 2022) (flagging but not deciding this issue). But because traditional financial institutions are necessarily subject to Gramm-Leach, that reading would render the Act’s mention of Gramm-Leach surplusage. To exempt only traditional financial institutions, section 25(c) could simply have read, “Nothing in this Act shall be deemed to apply in any manner to a financial institution”—full stop. Yet the Act goes out of its way to use the term “financial institution” in combination with Title V of Gramm-Leach, which in turn provides its own definition of that term. So section 25(c)’s exception applies to “financial institutions” *as defined by* Title V.

How, then, does Gramm-Leach define financial institutions? And does Pindrop count under that definition? Answering these questions requires a deep plunge into Gramm-Leach and its regulations.

3. *Pindrop is a “financial institution” under Gramm-Leach.* Enacted in 1999, Title V of Gramm-Leach was codified at 15 U.S.C. §§6801–27. Pub. L. No. 106-102, 113 Stat. 1436–50. The law was designed to “protect the security and confidentiality of ... nonpublic personal information” and authorizes several agencies to establish rules

ensuring that “financial institutions” keep personal financial information private. 15 U.S.C. §§ 6801, 6804. Title V’s definition section says that a financial institution is “any institution” whose business is to engage in any of the “financial activities” described in 12 U.S.C. § 1843(k), which regulates bank holding companies. 15 U.S.C. § 6809(3)(A).

Section 1843 generally bans bank holding companies from “engag[ing] in any activities other than ... those of banking or of managing or controlling banks.” 12 U.S.C. § 1843(a)(2). But subsection (k) carves out an exception: even if an activity cannot be considered “banking,” financial holding companies can still engage in it if the Federal Reserve determines it is “financial in nature or incidental to such financial activity.” § 1843(k)(1)(A). Subsection (k) gives further guidance. It lists activities that *are* “financial in nature,” including “any activity” that the Federal Reserve had determined by order or regulation (effective as of November 12, 1999) “to be so closely related to banking or managing ... banks as to be [considered] a proper incident” to banking. § 1843(k)(4)(F). Put together, if Pindrop can show such a Federal Reserve determination bearing on its current activities, then (1) those activities are financial under § 1843(k), (2) Pindrop is a financial institution subjected to Gramm-Leach, and (3) it is thus exempted under the Act.

Pindrop points me to a Federal Reserve order letting several bank holding companies engage in a joint technology venture that would establish a global authentication system for their customers. *See* 86. Fed. Res. Bull. 56, 57 (available at 2000 WL 49269). Among other things, the joint venture would register public and private keys

for encrypting and decrypting electronic communications, issue digital certificates for each unique key, and verify the validity of those digital certificates. *Id.* at 57–58. In its decision, the Federal Reserve Board found that “authenticating the identity of customers conducting financial and nonfinancial transactions [is an] activit[y] that [is] closely related to banking.” *Id.* at 59. Though this order was published in January 2000, it took effect on November 10, 1999. *Id.* at 61. And it is now codified at 12 C.F.R. §225.86(a)(2)(iii).

So, before November 12, 1999, the Federal Reserve had found that “authenticating the identity of persons conducting financial and nonfinancial transactions” was “so closely related to banking ... as to be [considered] a proper incident” to banking, and thus bank holding companies could engage in that activity. *Id.*; 12 U.S.C. §1843(k)(4)(F). And when Gramm-Leach was enacted to “protect the security and confidentiality of ... nonpublic personal information,” it applied its privacy regulations to “any institution” that engages in such authentication activity, whether it was a bank holding company or not. 15 U.S.C. §§6801(a), 6809(3)(A).

Pindrop’s authentication activities for John Hancock thus subject it to Gramm-Leach. John Hancock is an Amazon Connect customer that has paid for Pindrop’s authentication plug-in. D.I. 47 ¶¶64, 67–68, 98, 102. Plaintiffs called John Hancock to discuss their financial accounts. ¶¶98–101. Pindrop’s technology received call audio from Amazon, extracted plaintiffs’ voiceprints, analyzed those voiceprints, and confirmed their identity for John Hancock. ¶¶59–61, 78–80, 102–03. So plaintiffs allege that Pindrop performs the same activity as the joint venture described above:

“authenticating the identity of persons conducting financial and nonfinancial transactions.” 12 C.F.R. §225.86(a)(2)(iii).

4. *Gramm-Leach’s regulations also show that Pindrop is a “financial institution.”*

But there is more. Recall that the Act exempts financial institutions that are subject both to Gramm-Leach *and to the rules promulgated under it.* 740 Ill. Comp. Stat. 14/25(c). We have already seen that Pindrop meets Gramm-Leach’s statutory definition of a financial institution. Examining Gramm-Leach’s associated regulations confirms that the financial-institution exemption applies to Pindrop.

Take the so-called Regulation P (12 C.F.R. Part 1016), which was promulgated under Gramm-Leach and “governs the treatment of nonpublic personal information about consumers by ... financial institutions.” 12 C.F.R. §1016.1(a), (b)(1); *see also* §1016.3(s)(1). In defining its scope, the regulation says that it “applies to any financial institution ... that is subject to ... Title V of [Gramm-Leach].” §1016.1(b)(1). To further clarify who falls under that scope, the regulation elsewhere defines “financial institution” more thoroughly. *See* §1016.3(l). There, we find a special definition for entities that are both (1) described in 15 U.S.C. § 6805(a)(7) and (2) not described in 15 U.S.C. §6804(a)(1)(C). §1016.3(l)(3)(i). (Section 6804(a)(1)(C) refers to a “person described” in 12 U.S.C. §5519(a). Section 5519(a), in turn, refers to car dealers.) Pindrop checks both those boxes: (1) it is subject to the FTC’s enforcement jurisdiction because it is not listed in 15 U.S.C. §6805(a)(1)–(6) (and thus is described in §6805(a)(7)), and (2) is not a car dealer. *See* 15 U.S.C. §§6805(a)(7), 6804(a)(1)(C); 12 U.S.C. §5519(a).

The special definition is this: An entity is a “financial institution” under Regulation P if its “business ... is engaging in financial activities” described in 12 U.S.C. § 1843(k) (which we discussed above). 12 C.F.R. § 1016.3(l)(3)(i). And if it is “significantly engaged in financial activities,” it automatically counts. *Id.* The regulation then provides several examples of “financial institutions” under this special definition. § 1016.3(l)(3)(ii).

Those examples show that Pindrop meets this special definition of financial institution. For instance, a “retailer that extends credit by issuing its own credit card directly to consumers is a financial institution.” § 1016.3(l)(3)(ii)(A). That is because extending credit is one of the financial activities referred to by 12 U.S.C. § 1843(k)(4)(F), and simply offering credit cards means the retailer “is significantly engaged” in that financial activity. *Id.* That explanation proves Pindrop’s point. Pindrop provides authentication services for financial transactions, which, as we have seen, is one of the financial activities referenced by 12 U.S.C. § 1843(k)(4)(F). And authentication is a significant part of its business. D.I. 47 ¶¶ 57–63, 78–80, 98–107. Other examples confirm that if your business provides a service referred to in 12 U.S.C. § 1843(k)(4)(F), and that service is a significant part of your operations, your business must comply with Regulation P. *See, e.g.*, 12 C.F.R. § 1016.3(l)(3)(ii)(E). So Pindrop must comply with Regulation P.

And Regulation P is not the only regulation promulgated under Gramm-Leach that a business like Pindrop must follow. For example, 16 C.F.R. Part 314 sets standards for safeguarding consumers’ private information and was also promulgated

under Gramm-Leach. 16 C.F.R. § 314.1(a). Its definition of “financial institution” parallels Regulation P’s special definition discussed above, and it gives the same examples to illustrate that definition. § 314.2(h). So, accepting plaintiffs’ allegations as true, Pindrop also needs to comply with 16 C.F.R. Part 314.

* * * * *

This breadcrumb trail shows the following:

- Pindrop provides authentication services for banking.
- Before November 12, 1999, the Federal Reserve had decided that such authentication services are so closely related to banking as to be considered a proper incident to banking.
- So Pindrop performs a financial activity listed in 12 U.S.C. § 1843(k).
- Thus, Pindrop is a “financial institution” under Gramm-Leach and must follow its requirements.
- And Pindrop is also subject to regulations authorized by Gramm-Leach.

Thus, Pindrop is a “financial institution ... that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder,” and “[n]othing in [the] Act ... appl[ies] in any manner to” it. 740 Ill. Comp. Stat. 14/25(c). So I dismiss all claims against Pindrop.

III. ONE CLAIM AGAINST AMAZON SURVIVES

A. Plaintiffs also lack standing to bring Count I, Count III, or a claim for injunctive relief against Amazon

On to Amazon. Amazon does not challenge plaintiffs’ standing. But if standing is suspect, I must raise the issue myself. *See Boley v. Universal Health Servs., Inc.*, 36 F.4th 124, 130 (3d Cir. 2022).

It appeared to me that Pindrop’s standing arguments apply equally to Amazon. After all, those counts are brought against both Pindrop and Amazon and allege

similar facts. D.I. 47 ¶¶ 178–84, 194–201. So I asked for letter briefing on the issue. D.I. 68.

Plaintiffs say that they have standing to bring their claims against Amazon, and their arguments are generally the same as their arguments for standing to sue Pindrop. D.I. 70. Perhaps surprisingly, Amazon agrees that plaintiffs have standing. D.I. 69. (This may be because Amazon wants to avoid a remand of some of Plaintiffs’ claims to state court. *See Bryant*, 958 F.3d at 620 (defendant removed under the Class Action Fairness Act and argued for plaintiffs’ standing to avoid remand).) But I am not persuaded.

1. *Count I*. Recall Count I, which alleges a violation of section 15(a) of the Act. D.I. 47 ¶¶ 178–184. Plaintiffs say that Amazon possessed their biometric data without establishing a written policy or destroying their data according to section 15(a)’s deadlines. *Id.* As I explained, failing to establish a written policy is not enough for standing. And as with Pindrop, plaintiffs fail to allege particular facts showing that Amazon no longer needs that data, or that it has been three years since they last interacted with Amazon. *Id.* So without allegations that Amazon has unlawfully retained their data, plaintiffs lack standing.

Amazon says plaintiffs’ allegations here are enough. D.I. 69, at 1–3. They are not. Plaintiffs point out that Amazon shared their biometric data with others. D.I. 70, at 4. But again, the duty not to share comes from section 15(d); section 15(a) addresses the duty to destroy. Plaintiffs also say that Amazon’s “indefinite use of [their]

biometric data independently confers standing.” *Id.* But, as noted, they have failed to plead specific facts about such continued use.

2. *Count III.* The same goes for Count III. There, plaintiffs allege that Amazon profited from their biometric data in violation of section 15(c). D.I. 47 ¶¶ 194–201. But they do not allege that Amazon’s actions prevented them from otherwise profiting on their own biometrics, or that Amazon disclosed their private information to anyone other than John Hancock. *See Thornley*, 984 F.3d at 1246–47.

Amazon points me to a new case that it says “casts doubt on *Thornley*’s analysis.” D.I. 69, at 3. In *Kashkeesh v. Microsoft Corp.*, a district court recognized that an intermediate Illinois court had implicitly disagreed with *Thornley*’s interpretation of section 15(c). 2022 WL 2340876, at *3 (N.D. Ill. June 29, 2022) (discussing *Tims v. Black Horse Carriers, Inc.*, 184 N.E.3d 466 (Ill. App. Ct. 2021)). But the *Kashkeesh* court refused to find that the Illinois court’s interpretation of section 15(c) disturbed *Thornley*. *Id.* at *3–4.

Amazon asks me to interpret section 15(c)—which forbids selling, leasing, or trading in biometric data—as protecting a right against *publishing* such data. D.I. 69, at 3 (citing *Tims*, 184 N.E.3d at 472–73). But even if I adopted that interpretation, plaintiffs have not alleged publication. All they allege is that Amazon shared their call audio with Pindrop and communicated to John Hancock that their identities had been verified. D.I. 47 ¶¶ 69, 80, 98, 102. So Amazon did not publish any *biometric data*. And for the same reason, plaintiffs’ claim that Amazon “amplified the[ir] invasion of ... privacy ... by disseminating [their biometrics] to other people” is unfounded. D.I.

70, at 4 (alteration adopted, internal quotation marks omitted). So under either *Tims*'s broader reading or *Thornley*'s narrower reading of section 15(c), plaintiffs have failed to allege the requirements for standing.

3. *Injunctive relief.* Plaintiffs' request for an injunction against Amazon fails for the same reasons as against Pindrop. Plaintiffs have not sufficiently alleged that a violation of the Act is ongoing or imminent. As I have explained, their allegations that Amazon retains their biometric data are conclusory. And they do not allege that they are still John Hancock customers, that John Hancock still uses Amazon, that they still call or imminently intend to call an Amazon-run call center, or that Amazon currently fails to comply with the Act. *See* D.I. 47 ¶ 70 (alleging that Amazon now *requires* compliance with the Act).

Amazon says that a motion to dismiss is not the place to dismiss a prayer for injunctive relief. D.I. 69, at 4. But it cites no binding authority for that proposition. And *Lyons* makes clear that a plaintiff must have standing for a federal court to issue an injunction. 461 U.S. at 101; *see also Whole Woman's Health v. Jackson*, 142 S. Ct. 522, 530, 537, 539 (2021) (ordering lower court to dismiss injunctive-relief case against a defendant for lack of standing).

B. Amazon has not shown that the Act's financial-institution exception applies

Like Pindrop, Amazon also says that it can take advantage of the Act's financial-institutions exception. D.I. 51, at 7–9. But its arguments fall flat.

As we have seen, the Act exempts any "financial institution or an affiliate of a financial institution that is subject to Title V of" Gramm-Leach and its associated

regulations. 740 Ill. Comp. Stat. 14/25(c). Congress precisely defined a “financial institution” under Gramm-Leach. And other regulations have fleshed out that term’s meaning.

But unlike Pindrop, Amazon does not claim it is a financial institution under Gramm-Leach. Instead, its basic argument is that because John Hancock is a financial institution exempt from the Act, and because it provides services for John Hancock, it should also be exempt from the Act. D.I. 51, at 8–9. According to Amazon, excluding it from the Act would be “eminently rational,” and finding otherwise would be “absurd and unworkable.” *Id.* (internal quotation marks omitted).

Federal judges sitting in Delaware are not well positioned to determine the most eminently rational way for Illinois to regulate the in-state use of biometrics. But we can read statutes. Amazon points me to nothing in the Act that says that *service providers* for financial institutions are exempt from the Act’s requirements. *See* 14/25(c). Neither does it try to argue that it counts as an “affiliate of a financial institution.” Nor could it: an affiliate under Gramm-Leach is “any company that controls, is controlled by, or is under common control with another company.” 15 U.S.C. §6809(6). That does not describe Amazon’s relationship with John Hancock or Pindrop.

Amazon says that it cannot ensure that customers like John Hancock will follow the Act. D.I. 51, at 9. But according to plaintiffs, Amazon now does that very thing. D.I. 47 ¶ 70. And Amazon says that John Hancock, not Amazon, captured plaintiffs’ biometrics and then stored them on Amazon’s servers. D.I. 51, at 9. Not so. Accepting the Complaint as true, Amazon captures voiceprints and authenticates callers itself.

D.I. 47 ¶¶ 69. Plus, unlike Pindrop, Amazon does not argue that its authentication activity makes it a financial institution under Gramm-Leach.

So Amazon has not shown that it can qualify for the Act’s financial-institution exception.

C. Count II survives, but Count IV fails to state claims against Amazon

I am dismissing Counts I and III for lack of standing. Amazon says I should dismiss the two other counts for failing to state a claim. Count II does state a claim under the Act. But Count IV does not.

Count II is based on section 15(b) of the Act. D.I. 47 ¶¶ 185–193. Section 15(b) bans “collect[ing]” biometric data without first getting written informed consent. Amazon says I should dismiss this count because John Hancock collected the biometric data, not Amazon. D.I. 51, at 10–11. But plaintiffs allege that Amazon itself extracts voiceprints and uses them to authenticate callers, all without informed consent. D.I. 47 ¶¶ 69, 93. So their section 15(b) claim survives.

But the outcome is different for Count IV. Plaintiffs say that Amazon shared their biometric data in violation of section 15(d). D.I. 47 ¶¶ 202–07. Yet the Complaint does not allege facts supporting this claim.

Here we must pay close attention to the Act’s definitions. Under the Act, a “biometric identifier” is simply a generic term given to six items, including voiceprints. 14/10. “Biometric information” is information derived from biometric identifiers that can be used to identify an individual. *Id.*

To state a claim for a section 15(d) violation, plaintiffs must allege that Amazon disclosed, redisclosed, or otherwise disseminated their biometric identifiers or

biometric information. 14/15(d). Plaintiffs say Amazon did that by sharing their voice audio with Pindrop. D.I. 56, at 19. But under the Act's terms, voice audio alone is neither a biometric identifier (a voiceprint) nor biometric information (information derived from a voiceprint). Plaintiffs also say they alleged that Amazon shared their biometric identifiers and information with John Hancock and other end users of Amazon Connect. *Id.* at 19–20 (citing D.I. 47 ¶¶ 71–74, 77, 80, 84–86, 90, 123, 132). But the Complaint nowhere alleges that Amazon shared plaintiffs' voiceprints, or that it shared any information based on voiceprints that could be used to identify them. The portions of the Complaint that plaintiffs cite refer only to Amazon's processes for authenticating callers on behalf of Amazon Connect customers like John Hancock. Although Amazon may have used plaintiffs' biometric identifiers and information to perform its own authentication services, the Complaint says only that Amazon communicated to its customers that plaintiffs were in fact who they said they were. It does not imply that Amazon shared their sensitive biometric data with anyone. So Count IV fails.

IV. OPPORTUNITY TO AMEND

Because I am dismissing Counts I and III for lack of standing, that dismissal is without prejudice. *See Thorne v. Pep Boys Manny Moe & Jack Inc.*, 980 F.3d 879, 896 (3d Cir. 2020).

Plaintiffs' remaining claims against Pindrop fail due to the Act's financial-institution exception. Because Pindrop's allegedly unlawful activity—providing authentication services for John Hancock—is what qualifies it for this exception, I am concerned

that amendment will be futile. So if plaintiffs wish to amend, they must file a motion for leave to amend.

Count II against Amazon may proceed. And because this is the first opinion to evaluate Count IV on the merits, I will not require a motion for leave to amend against Amazon. *See McGoveran v. Amazon Web Servs., Inc.*, 488 F. Supp. 3d 714 (S.D. Ill. 2020) (No. 3:20-cv-00031-NJR), ECF No. 67; D.I. 34, 35; Fed. R. Civ. P. 15(a)(2).

* * * * *

Most of plaintiffs' claims fall short, either for lacking standing or failing to state a claim. So I will dismiss all claims except Count II against Amazon.