UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
CENTRAL DIVISION at LEXINGTON

METTEKJISTINE MCKENZIE, *et al.*,	)	
	)	
	)	Case No.
Plaintiffs,	)	5:18-cv-359-JMH
	)	
v.	)	**MEMORANDUM OPINION**
	)	**AND ORDER**
ALLCONNECT, INC.,	)	
	)	
Defendant.	)	
	)	

***

An unsuspecting employee of Defendant Allconnect, Inc., responded to a fraudulent phishing email, resulting in an unauthorized release of employee W-2 tax forms, including sensitive personal information contained within those forms. The named Plaintiffs are former employees of Allconnect who allege that they, and other similarly situated employees, were harmed by the unauthorized release of their personally identifable information ("PII").

In response to this lawsuit, the Defendant argues that the Defendants lack standing because they have not alleged an actual injury in fact. Furthermore, the Defendant claims that the Plaintiffs have failed to properly plead claims upon which relief may be granted. Finally, and in the alternative, the Defendant moves to strike the class allegations from Plaintiffs' complaint. For the reasons that follow, Allconnect's motion to dismiss, and

motion to strike the class allegations, [DE 5] is **GRANTED IN PART** and **DENIED IN PART**.

First, Allconnect's motion to dismiss for lack of Article III standing is denied because the Plaintiffs have provided sufficient factual information to demonstrate that they suffered financial loss, lost time, and emotional distress as a result of the unauthorized release of their personal information.

Second, Allconnect's motion to dismiss Plaintiffs' claims for negligence, invasion of privacy based on intrusion upon seclusion, and breach of implied contract is denied because the Plaintiffs have pleaded sufficient information to meet federal pleading standards for these claims. Still, Plaintiffs' claims for invasion of privacy based on unreasonable publicity and for breach of fiduciary duty must be dismissed for failure to state claims upon which relief may be granted based on Rule 12(b)(6).

Third, and finally, the Court does not have sufficient information to adequately address the class certification issue at present. As such, the Court will allow limited discovery on factual issues relevant to class certification and will address class certification when the Plaintiffs raise the issue in a proper motion to certify the class.

I. Procedural History and Factual Allegations

For the purposes of this motion to dismiss, the factual allegations in Plaintiffs' complaint are treated as true and viewed

in the light most favorable to the Plaintiffs. Still, most of the relevant facts at this juncture do not appear to be in dispute.

Defendant Allconnect is a company that connects consumers with offers for internet services, television, home security, electricity, and other products. Allconnect operates multiple offices across the United States, including sales and customer care centers in Georgia, Kentucky, Texas, and Utah. [DE 1-1 at 5, Pg ID 13].

Plaintiffs Mettekjistine McKenzie and Chasity Combs are former employees of Allconnect. McKenzie is a resident of Arizona and was employed at Allconnect's Utah-based call center in 2016 and 2017. [*Id.* at 8, Pg ID 16]. Combs is a resident of Kentucky and worked at Allconnect's Kentucky-based call center from 2014 until 2018. [*Id.* at 9, Pg ID 17].

On February 14, 2018, an unknown individual impersonating Steven Sibley, the president of Allconnect, contacted an Allconnect employee through email and requested 2017 W-2 information for all Allconnect employees. [*Id.* at 6, Pg ID 14]. Likely believing that the email message was actually from Sibley, the Allconnect employee sent a data file containing Allconnect employees' W-2 information, including employees' names, addresses, social security numbers, and wage information. [*Id.* at 6, 11, Pg ID 14, 19].

Of course, it turns out that the email sent to the unsuspecting Allconnect employee was not from Allconnect's president and the data file sent in response was sent to cybercriminals perpetuating a fraud to gain the personal information of Allconnect's employees. On or around March 28, 2018, Allconnect discovered the unauthorized data disclosure. [*Id.* at 6, Pg ID 14]. In response, on April 2, 2018, Allconnect emailed former and current employees informing them about the data disclosure. [*Id.* at 5-6, Pg ID 13-14]. Additionally, Allconnect mailed letters to affected employees on April 2, 2018. [*Id.*]. Finally, Allconnect agreed to provide affected employees with two years of complimentary identity protection services through Allclear ID. [*Id.* at 11, Pg ID 19].

Plaintiffs claim that they, and other similarly affected Allconnect employees have been damaged by the unauthorized disclosure of their personal data. The Plaintiffs argue that they must take measures to "both deter and detect identity theft." [*Id.* at 6, Pg ID 14]. For instance, Plaintiffs claim that time spent on efforts to mitigate the harm from the data disclosure would otherwise be dedicated to different professional and personal activities. [*Id.*]. Moreover, the Plaintiffs argue that they have suffered lost time and damages as a result of having to place freezes and alerts on their credit reports with credit reporting agencies, have had to close or modify financial accounts, contact

their financial institutions, and closely monitor their reports, among other mitigating activities. [*Id.* at 6-7, Pg ID 14-15].

As a result, the Plaintiffs filed a lawsuit in Fayette Circuit Court. [DE 1-1]. The action was removed to this Court by Allconnect based on minimal diversity of citizenship pursuant to the Class Action Fairness Act of 2005 ("CAFA"). [DE 1]. Subsequently, Defendant Allconnect moved to dismiss Plaintiffs' complaint for lack of standing, failure to state claims upon which relief may be granted, and, in the alternative, moved to strike the class allegations in the complaint. [DE 5]. The Plaintiffs responded in opposition [DE 20] and the Defendant replied [DE 22], making this matter ripe for review.

III. Analysis and Standard of Review

Plaintiffs bring four causes of action against Allconnect on behalf of the entire class, they are, (1) negligence, (2) invasion of privacy, (3) breach of implied contract, and (4) breach of fiduciary duty. The Defendant claims that the compliant must be dismissed. First, the Defendant argues that the Plaintiffs lack standing to bring this lawsuit because they have not alleged an injury in fact. Second, the Defendant argues that the Plaintiffs have failed to plead sufficient factual information upon which relief may be granted. Finally, and in the alternative, the Defendant asks the Court to strike the class allegations in the complaint if any of the claims survive.

A. Article III Standing

First, Allconnect claims that the Plaintiffs have failed to establish a sufficient injury in fact to establish a cognizable Article III injury. [DE 5-1 at 4-7, Pg ID 63-66]. More specifically, the Defendant argues that apprehension of future injury as a result of the data breach, without more, is insufficient to create standing. [*Id.* at 5-6, Pg ID 64-65].

"Article III of the Constitution limits the jurisdiction of federal courts to 'Cases' and 'Controversies,'" and "[t]he doctrine of standing gives meaning to these constitutional limits by 'identify[ing] those disputes which are appropriately resolved through the judicial process.'" *Susan B. Anthony List v. Driehaus*, 573 U.S. 149 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992)). "To establish Article III standing, a plaintiff must show (1) an 'injury in fact,' (2) a sufficient 'causal connection between the injury and the conduct complained of,' and (3) a 'likel[ihood]' that the injury 'will be redressed by a favorable decision.'" *Id.* (quoting *Lujan*, 504 U.S. at 560–561 (internal quotation marks omitted)).

But here, Allconnect expressly acknowledges that a split panel of the United States Court of Appeals for the Sixth Circuit held that Article III standing existed in a similar data breach situation. *Galaria*, 663 F. App'x at 388. In *Galaria*, the Sixth

Circuit was faced with a situation like the one at bar where Nationwide employees filed a putative class action after a data breach resulted in the unauthorized release of employees' personal data. The Defendant, Nationwide, argued in part that the plaintiffs did not have Article III standing because they had not alleged a cognizable injury as a result of the data breach.

The majority in *Galaria* acknowledged that courts have reached different conclusions on whether plaintiffs had alleged a cognizable injury in data breach situations to confer Article III standing but ultimately concluded that "[p]laintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation." *Id.* at 388-89 (discussing the circuit split and citing cases). In so holding, the *Galaria* court said, "[A]lthough it might not be literally certain that Plaintiffs' data will be misused . . . there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable" and that "these costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing." *Id.*

Still, the dissenting judge in *Galaria* stated that the court "need not take sides in the existing circuit split regarding whether an increased risk of identity theft is an Article III injury because, even assuming that it is, the plaintiffs have

failed to demonstrate the second prong of Article III standing—causation." *Id.* at 392. The dissent would not have reached the Article III issue and instead would have held that the plaintiffs had failed to demonstrate the requisite causal connection between Nationwide's activity and the conduct of third-party hackers that stole employees' personal information. *Id.* at 393.

The *Galaria* decision is technically not binding on this Court since it is an unpublished and non-precedential opinion of the Sixth Circuit. *See Plumley v. Austin*, 135 S.Ct. 828, 831 (2015) (Thomas, J. and Scalia, J. dissenting) ("[T]he decision below is unpublished and therefore lacks precedential force."); Fed. R. App. P. 32.1; 6 Cir. R. 32.1.

Still, Allconnect seems to acknowledge that the *Galaria* decision is highly persuasive on the issue of standing but "respectfully submit[s] that *Galaria*'s holding appears inconsistent with *Clapper*'s[1] standard and therefore, is incorrectly decided." [DE 5-1 at 6, Pg ID 65]. But Allconnect has not attempted to distinguish the *Galaria* holding from this case in a meaningful way. In fact, the *Galaria* court held that Article III standing existed in a data breach situation that is very similar to the case at bar.

[1] The full citation to the *Clapper* decision referenced in the direct quote in text is *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).

Here, applying the logic in *Galaria*, the Plaintiffs have demonstrated that they had to take reasonable steps to mitigate damages from the unauthorized release of their PII to unknown phishing scammers. The Plaintiffs have provided factual information that demonstrates that they have lost time and money as a result of taking steps to protect their personal data and prevent the misuse of that data by scammers. At the very least, the Plaintiffs' mitigation efforts constitute a cognizable injury that is a direct result of the unauthorized release of employees' PII by Allconnect. As such, the Plaintiffs have alleged a sufficient injury in the form of mitigation costs to prevent the misuse of their stolen personal information and have allege a sufficient Article III injury.

As a result, at the pleading stage, the Plaintiffs in this case have demonstrated Article III standing by alleging that the unauthorized release of their personal data has resulted in a substantial risk of harm paired with mitigation costs. The Court notes that Allconnect argues that *Galaria* was incorrectly decided but Allconnect has not made any effort to distinguish Galaria from the present case. As a result, any arguments directly attacking the propriety of the holding in *Galaria* must be presented to the Sixth Circuit, not this Court. Regardless, at the pleading stage, Plaintiffs have provided enough information to demonstrate that they lost time and money, in addition to suffer emotional distress,

as a result of the unauthorized release of personal data, which constitutes a cognizable injury that is sufficient to confer Article III standing.

B. Motion to Dismiss Based on Rule 12(b)(6)

Second, Allconnect argues that Plaintiffs' claims must be dismissed under Federal Rule of Civil Procedure 12(b)(6) for failure to state claims upon which relief may be granted based on federal pleading standards.

In diversity cases, while the Court must apply the substantive law of the forum state, the federal pleading standards apply. *See* Fed. R. Civ. P. 81(c)(1); *Granny Goose Foods, Inc. v. Bhd. of Teamsters and Auto Truck Drivers*, 415 U.S. 423, 438 (1974) (applying the Federal Rules of Civil Procedure to removed actions); *see also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). A plaintiff's complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). While the plaintiff must provide sufficient facts to support his claims, he or she need not provide every fact that may be raised at trial. *See Scheid v. Fanny Farmer Candy Shops, Inc.*, 859 F.2d 434, 436–37 (6th Cir. 1988) ("[A] complaint must contain either direct or inferential allegations respecting all the material elements to sustain a recovery under some viable legal theory." (internal quotation marks omitted)).

A motion to dismiss under Rule 12(b)(6) tests the sufficiency of the plaintiff's complaint. "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of the cause of action will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal citations omitted). The complaint must make factual allegations that, when accepted as true, state a plausible claim for relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* When considering plausibility, the court construes the complaint in the light most favorable to the plaintiff. *Strayhorn v. Wyeth Pharms., Inc.*, 737 F.3d 378, 387 (6th Cir. 2013).

The parties make some mention of the applicable law in this matter since the class representatives were employed by Allconnect in different states. Of course, choice of law rules constitute the substantive law of a state and federal courts are obliged to apply state choice of law rules in diversity actions. *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 495-98 (1941).

Thus, at some point, the Court will need to engage in a choice of law analysis in this matter but that is not necessary at this

stage of this putative class action. At present, the parties appear to agree that the two class representatives allege harms that occurred in Kentucky and Utah respectively. While the parties mention choice of law in a conclusory manner, the Court does not have sufficient information at this juncture to engage in a comprehensive choice of law analysis. As a result, for the purposes of this 12(b)(6) motion to dismiss, the Court will consider the pleaded claims under the substantive law of both Kentucky and Utah.

(1) Negligence

Allconnect argues that the Plaintiffs have failed to properly plead a claim for negligence in two ways. First, Allconnect claims that it does not have a duty, as a matter of law, to protect its employees from harm from third-party actors and cybercriminals. Second, Allconnect claims that the Plaintiffs have not demonstrated a cognizable injury.

The elements of a claim for negligence are similar under both Kentucky and Utah law. As a general matter, the elements of negligence, familiar to all attorneys and law students, are, (1) that defendant owed the plaintiffs a duty of care, (2) that defendant breached the applicable duty of care, (3) causation, including both cause in fact and proximate cause, and (4) that the plaintiff was damaged by the breach of the duty of care. *See, e.g.*, *Keaton v. G.C. Williams Funeral Home, Inc.*, 436 S.W.3d 538,

542 (Ky. Ct. App. 2013); *Hunsaker v. State*, 870 P.2d 893, 897 (Utah 1993).[2]

As to Allconnect's first contention, Allconnect may be correct that it does not owe its employees a duty to protect them from unknown third parties or thieves but that does not entirely address Plaintiffs' claim for negligence. Allconnect has cited numerous cases that stand for the legal principle that there is no common law duty to protect persons from harm caused by unknown third parties in a data breach situation like this one.

Still, Allconnect's argument does not comprehensively capture Plaintiffs' claim for negligence here. The Plaintiffs claim that Allconnect had a duty to safeguard the sensitive personal information that employees were obligated to provide Allconnect as conditions of their employment. This is not a case where the Plaintiffs claim that Allconnect was responsible solely for the actions of unknown third-party cybercriminals. Here, the Plaintiffs claim that the Defendant had a duty to take reasonable steps to safeguard their personal information.

[2] Some Kentucky courts express the elements of negligence differently, but they are substantively the same. Some Kentucky courts express three elements for proving a negligence claim, they are, "1) duty; 2) breach of that duty; and 3) consequent injury." *Keaton*, 436 S.W.3d at 542 (citing *Mullins v. Commonwealth Life Ins. Co.*, 839 S.W.2d 245, 247 (Ky. 1992)). The third element, consequent injury, includes two distinct elements—actual injury and legal causation between the breach and the injury. *Id.* (citing *Pathways, Inc. v. Hammons*, 113 S.W.3d 85, 88–89 (Ky. 2003)).

To that end, when accepting the facts as true and reading the complaint in the light most favorable to the Plaintiffs, the Plaintiffs have provided sufficient information at this stage to survive a motion to dismiss on the duty of care element. The Plaintiffs have provided sufficient information in the complaint to demonstrate that they were obligated to provide sensitive personal information to Allconnect as a condition of their employment. As a result, while Allconnect may not have had a duty to protect its employees from unknown or unforeseen third-parties, Allconnect did have a duty to prevent foreseeable harm to its employees and, as part of that duty, had a duty to safeguard the sensitive personal information of its employees from unauthorized release or theft. Of course, that is not to say that the Plaintiffs have demonstrated that the duty was breached in this case but only that, when reading the complaint in the light most favorable to the Plaintiff and assuming the facts as true, that the Plaintiffs have pleaded sufficient factual information in their complaint to demonstrate they were owed a duty of care.

Allconnect's second argument, that the Plaintiffs have not demonstrated a cognizable injury, is largely a reiteration of Allconnect's argument against Article III standing. Allconnect claims that the Plaintiffs' damages are completely speculative and conjectural injuries that may or may not occur sometime in the future. While Allconnect's point may go to the appropriate amount

of damages in this action, at this stage, the Plaintiffs have pleaded sufficient information to demonstrate that they have suffered a cognizable injury related to their negligence claim.

Initially, there is no dispute that an unauthorized data release occurred in this case that resulted in Plaintiffs' personal information being released to unknown third-parties as a result of an email phishing scam. As a result of that breach, Plaintiffs have alleged that they have suffered monetary loss as a result of efforts to safeguard their information after the unauthorized data release. Furthermore, in addition to other damages, Plaintiffs aver that they have suffered emotional distress as a result of the breach and have lost time and money as a result of past and continued efforts to protect their personal information and prevent the unauthorized use of their personal information. Again, Plaintiffs may not ultimately be successful on the element of injury or damages. Regardless, at the pleading stage, the Plaintiffs have provided sufficient factual information to demonstrate that they may have suffered damages as a result of the unauthorized data release.

In sum, after accepting all the facts in the complaint as true and reading the complaint in the light most favorable to the Plaintiffs, the Plaintiffs have provided sufficient information in the complaint to plead a claim for negligence. As a result,

Allconnect's motion to dismiss Plaintiffs' negligence claim must be denied.

(2) Invasion of Privacy

Invasion of privacy may consist of four distinct torts: (1) unreasonable intrusion upon seclusion; (2) misappropriation of another's name of likeness; (3) unreasonable publicity given to one's private life; and (4) publicity that places another in a false light. *See, e.g.*, *Pearce v. Whitenack*, 440 S.W.3d 392, 400 n.5 (Ky. Ct. App. 2014) (citing *McCall v. Courier–Journal & Louisville Times Co.*, 623 S.W.2d 882, 887 (Ky. 1981) (adopting Restatement (Second) of Torts § 652A (Am. Law Inst. 1977))); *Stein v. Marriott Ownership Resorts, Inc.*, 944 P.2d 374, 377-78 (Utah 1997). Only intrusion upon seclusion and unreasonable publicity appear to be at issue here based on the parties' briefing.

i. Intrusion Upon Seclusion

Both Kentucky and Utah comply with the Restatement (Second) of Torts on the elements for a claim of intrusion upon seclusion. *See* Restatement (Second) of Torts: Privacy § 652B (Am. Law Inst. 1977). The elements for a claim of intrusion upon seclusion are, (1) an intentional intrusion by the defendant, (2) into a matter that the plaintiff has a right to keep private, and (3) which is highly offensive to a reasonable person. *Pearce*, 440 S.W.3d at 400-01; *Judge v. Saltz Plastic Surgery, PC*, 330 P.3d 126, 136 (Utah Ct. App. 2014).

Allconnect argues that the Plaintiffs have not alleged sufficient facts to demonstrate that the Allconnect intentionally intruded upon Plaintiffs' seclusion. In response, the Plaintiffs contend that Allconnect acted with reckless disregard for Plaintiffs' privacy when "Allconnect improperly accessed the data file containing its employees' PII and sent the file to cyber criminals."

At this stage, the Plaintiffs have provided enough factual content to plead a claim for intrusion upon seclusion. The Plaintiffs allege that an employee of Allconnect took an affirmative action to gather the tax information for Allconnect employees and send it in response to a fraudulent email. The allegation that the employee gathered employees' data constitutes sufficient factual information to plead an intrusion.

Of course, it appears that this employee thought he or she was sending the information to Allconnect's president and not to third-party tricksters but that does not conclusively demonstrate that the Defendant's employee did not act intentionally. A defendant's actions may be intentional when the Defendant acts with such reckless disregard for the privacy of the plaintiff that the actions rise to the level of being an intentional tort. *See Smith v. Bob Smith Chevrolet, Inc.*, 275 F. Supp. 2d 808, 822 (W.D. Ky. 2003).

In this case, the Plaintiffs have provided factual information, that when accepted as true, demonstrates that the Defendant was aware of the potential hazard posed by phishing scams, failed to adequately train their employees or implement appropriate policies to prevent the unauthorized release of employees' data, and that Allconnect did in fact release the data of employees to third parties. This information, when read in the light most favorable to the Plaintiffs, demonstrates that the Plaintiffs have properly pleaded a claim for intrusion upon seclusion. Of course, that is not to say that the Plaintiffs will ultimately prevail on this cause of action. But, at this stage, the Plaintiffs have provided sufficient factual content to meet federal pleading standards on the tort of intrusion upon seclusion and Allconnect's motion to dismiss Plaintiffs' claim for intrusion upon seclusion must be dismissed.

ii. Unreasonable Publicity

Both Kentucky and Utah appear to follow the Restatement (Second) of Torts on the discrete tort of unreasonable publicity. *See Savidge v. Pharm-save, Inc.*, No. 3:17-cv-186-TBR, 2017 WL 5986972, at *8 (W.D. Ky. Dec. 1, 2017); *Stein*, 944 P.2d at 380. At this juncture, the issue is whether the Plaintiffs have alleged that Allconnect *published* their private information. The Restatement says that "'[p]ublicity' . . . means that the matter is made public, by communicating it to the public at large, or to

so many persons that the matter must be regarded as substantially certain to become one of public knowledge." Restatement (Second) of Torts: Privacy § 652D cmt. a (Am. Law Inst. 1977).

Here, the Plaintiffs have failed to demonstrate that Allconnect communicated their private information to the public at large or to so many persons that the matter must be regarded as substantially certain to become public knowledge. Cases addressing similar data breaches have concluded that unauthorized disclosure of personal information does not constitute publication. *See Savidge*, 2017 WL 5986972 at *9; *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 662-63 (S.D. Ohio 2014), *overruled on other grounds by* 663 F. App'x 384 (6th Cir. 2016).

The Plaintiffs attempt to distinguish *Savidge* and save their claim by arguing that this case is different because an Allconnect employee "voluntarily provided" employees' information to cybercriminals and "personally shared PII with unknown individuals of the public who intend to further circulate it for illicit purposes." [DE 20 at 16, Pg ID 147]. But Plaintiffs' argument on this point constitutes an expansion of the legal meaning of publicity masquerading as a distinction. It is true that this case is slightly different factually from the cited cases because an Allconnect employee provided the personal information in response to a phishing email as opposed to the information being

hacked. Still, there is no allegation in the complaint about how many persons had access to the email address where the personal information of Allconnect employees was sent. Furthermore, there is no allegation that any of the employees' personal information has been widely disseminated to the public. Simply put, the Plaintiffs have failed to provide any factual information about how many people have access to their data or if that data has been posted widely online.

As a result, the Plaintiffs have failed to demonstrate that Allconnect published their private data. Of course, the unknown scammers may disseminate or sell the employees' personal information. Still, if the scammers disseminate the private information of the employees, they will be publishing this information, not Allconnect. Ultimately, holding that Allconnect published the private information of its employees by unknowingly responding to a phishing email would be inconsistent with other cases that have held to the contrary and would expand the term publish beyond both its natural and legal meaning in this context. As such, Plaintiffs' claim for invasion of privacy based on unreasonable publicity must be dismissed.

(3) Breach of Implied Contract

To establish breach of an implied contract, the Plaintiff must prove the existence of an implied contract, created by mutual assent, and the failure of a party to comply with the contract's

terms. *See Furtula v. University of Kentucky*, 438 S.W.3d 303, 308-09 (Ky. 2014); *Retherford v. AT&T Commc'ns of Mountain States, Inc.*, 844 P.2d 949, 967 (Utah 1992).

Allconnect argues that the Plaintiffs have failed to demonstrate that a meeting of the minds existed to create an implied contract. Moreover, Allconnect claims that even if there was an implied contract that Plaintiffs' claim must be dismissed for failure to allege actual damages.

First, Allconnect argues that Plaintiffs raise conclusory allegations that fail to demonstrate that there was a sufficient meeting of the minds to imply a contract that Allconnect would protect employees' information from unknown hackers. This argument parallels arguments raised by Allconnect while asserting that they owed no duty to protect the Plaintiffs from hackers.

Regardless, at this stage in the litigation, the Plaintiffs have provided enough factual information to plead a claim for an implied contract. The Plaintiffs do not claim that Allconnect impliedly contracted to protect them from unforeseen criminals and hackers. Instead, the Plaintiffs allege that "[i]mplicit in the employment agreement between Allconnect and its employees was the *obligation that both parties would maintain information confidentially and securely*." [DE 1-1 at 30, Pg ID 38 (emphasis added)]. To that end, the Plaintiffs allege that they entered into employment agreements with Allconnect, that as a condition of

their employment they had to provide personal information to Allconnect, and that Allconnect implicitly agreed to safeguard that information. This is sufficient at the pleading stage for the implied contract claim to survive.

This conclusion is on point with similar federal cases that have found an implied contract by an employer to protect the personal information of employees in data breach situations. *See, e.g.*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 158-59 (1st Cir. 2011) ("The district court correctly concluded that a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use the credit card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information."); *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *16 (N.D. Ga. Mar. 5, 2018) (noting that "[s]everal federal courts have recognized implied-in-fact contract claims in data breach cases" and citing cases); *Savidge*, 2017 WL 5986972, at *9; *Castillo v. Seagate Tech., LLC*, No. 16-cv-01958-RS, 2016 WL 9280242, at *8-9 (N.D. Cal. Sept. 14, 2016).

Allconnect's rather perfunctory response that some of the previously mentioned cases were wrongfully decided and that the Plaintiffs have failed to allege sufficient information in their complaint to plead that a meeting of the minds occurred is unavailing. Allconnect claims that *Savidge* and *Castillo* were

incorrectly decided based on the holding in *Longenecker-Wells v. Benecard Services, Inc.*, 658 F. App'x. 659, 662 (3d Cir. 2016). Of course, there are cases that have failed to hold that an implied contract existed in similar situations to the case at bar. *See In re Arby's Rest. Grp. Inc. Litig.*, 2018 WL 2128441, at *16 n.17 (citing cases). Still, the cases to the contrary cited by Allconnect are only persuasive authority for this Court.

Additionally, and more importantly, the crucial distinction in this case is that an Allconnect employee inadvertently sent the personal data of Allconnect employees to unknown persons by falling prey to a phishing email. This case is not one where third-party hackers acting on their own invaded the personal data of Allconnect's employees. Instead, an Allconnect employee unintentionally played a direct role in the breach by responding to a trickster's email. As a result, even if Allconnect had not impliedly agreed to protect employees from unknown hackers, the Plaintiffs have alleged sufficient information to demonstrate that Allconnect implicitly agreed to take reasonable precautions to safeguard the personal data of employees.

Finally, Allconnect makes a familiar and mechanical argument, claiming that Plaintiffs' claim for breach of implied contract must be dismissed because the Plaintiffs have failed to allege any actual damages as a result of the data disclosure. Of course, it may be the case that the Plaintiffs fail to demonstrate actual

damages upon which they may recover for an implied breach of contract. Still, at this stage, accepting the facts pleaded in the complaint as true and reading the complaint in the light most favorable to the Plaintiffs, the Plaintiffs have alleged sufficient factual information to plead damages as a result of the data breach, including lost time and wages as a result of efforts to protect their personal data, emotional distress, and monetary loss as a result of efforts to mitigate damages arising from the unauthorized disclosure.

In sum, the Plaintiffs have provided sufficient factual information to plead a claim for breach of an implied contract and Allconnect's motion to dismiss this claim is denied.

(4) Breach of Fiduciary Duty

Fourth, and finally, the Plaintiffs pleaded a claim for breach of fiduciary duty. The Defendants contend that the Plaintiffs do not allege a fiduciary relationship between Allconnect and the Plaintiffs in this context.

A fiduciary relationship is one "founded on trust or confidence reposed by one person in the integrity and fidelity of another and which also necessarily involves an undertaking in which a duty is created in one person to act primarily for another's benefit in matters connected with such undertaking." *ATC Distrib. Grp., Inc. v. Whatever It Takes Transmissions & Parts, Inc.*, 402 F.3d 700, 715 (6th Cir. 2005) (quoting *Steelvest, Inc. v. Scansteel*

Serv. Ctr., Inc., 807 S.W.2d 476, 485 (Ky.1991)); *accord First Sec. Bank of Utah N.A. v. Banberry Dev. Corp.*, 786 P.2d 1326, 1333 (Utah 1990).

In this case, Allconnect likely had some duty to take reasonable steps to protect the private information provided by employees, but that does not indicate that a fiduciary relationship existed between Allconnect and its employees in this context. The Plaintiffs claim that "Allconnect was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiffs and Class members, for the safeguarding of employees' PII and wage information." [DE 1-1 at 32, Pg ID 40]. Furthermore, the Plaintiffs contend that "Allconnect had a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their employer/employee relationship, in particular to keep secure income records and the PII of its employees." [*Id.*]. But the Plaintiffs' allegations on this point constitute unsupported legal conclusions.

In Plaintiffs' response in opposition to Allconnect's motion to dismiss, Plaintiffs cite two cases where they say Kentucky and Utah has recognized a fiduciary relationship between an employer and an employee. It is true that employer-employee relationships are one of the "[c]ommon examples of fiduciary relationships." *Mohnsam v. Nemes*, No. 3:17-cv-00427-CRS, 2018 WL 1041305, at *2

(W.D. Ky. Feb. 23, 2018); *accord Prince, Yeates & Geldzahler v. Young*, 94 P.3d 179, 184-85 (Utah 2004). Regardless, none of the cases cited by the Plaintiffs suggest that a fiduciary relationship exists between an employer and employees in the context of protecting employees' private data.

Furthermore, most cases, including the cases cited by the Plaintiffs, have discussed the fiduciary relationship between employers and employees in the context of a limited *fiduciary duty owed by the employee*, as an agent of the employer, not to compete and to be loyal to the employer. *See Johnson v. Brewer & Pritchard, P.C.*, 73 S.W.3d 193, 199-200 (Tex. 2002); *see also* Restatement (Third) of Agency § 8.01 cmt. c (Am Law. Inst. 2006) ("All who assent to act on behalf of another person and subject to that person's control are common-law agents as defined in § 1.01 and are subject to the general fiduciary principle stated in this section. Thus, the fiduciary principle is applicable to gratuitous agents as well as to agents who expect compensation for their services, and to employees as well as to nonemployee professionals, intermediaries, and others who act as agents.").

Simply put, the law does not support Plaintiffs' contention that a fiduciary relationship existed between Allconnect and Allconnect employees in relation to securing the personal information of employees. The Plaintiffs engaged in an employment relationship with Allconnect, but that fact alone is insufficient

to prove that a fiduciary relationship existed. Here, the Plaintiffs have failed to provide sufficient factual information in the complaint to suggest that Allconnect expressly undertook, formally or informally, a duty to act for employees' benefit in this context. *See Flegles, Inc. v. TruServ Corp.*, 289 S.W.3d 544, 552 (Ky. 2009) ("A fiduciary, moreover, is one who has expressly undertaken to act for the plaintiff's primary benefit. . . . Although fiduciary relationships can be informal, a fiduciary duty does not arise from the universal business duty to deal fairly nor is it created by a unilateral decision to repose trust and confidence."). Allconnect may have owed a duty to take reasonable steps to protect the personal information of employees, but the Plaintiffs have failed to plead a claim that demonstrates that the employer-employee relationship may have risen to the level of a fiduciary relationship in this context. As a result, Plaintiffs' claim for breach of fiduciary duty must be dismissed.

C. Striking the Class Allegations

In their complaint, Plaintiffs state that they seek to bring this suit as a class action on behalf of all Allconnect employees whose PII was compromised as a result of the unauthorized data disclosure. [DE 1-1 at 21-25, Pg ID 29-33]. In its motion to dismiss, Allconnect states that the class allegations in the complaint must be stricken because the Plaintiffs cannot satisfy the Rule 23 requirements for class certification.

At this juncture, the Plaintiffs have not moved for class certification. The Federal Rules provide that a certification order should issue "[a]t an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action." Fed. R. Civ. P. 23(c)(1)(A).

Still, at this stage in the litigation, before any limited discovery, it is premature to decide the class certification issue. *See In re Am. Med. Sys., Inc.*, 75 F.3d 1069, 1079 (6th Cir. 1996) ("[O]rdinarily the determination should be predicated on more information than the pleadings will provide. . . . The parties should be afforded an opportunity to present evidence on the maintainability of the class action.") (quoting *Weathers v. Peters Realty Corp.*, 499 F.2d 1197, 1200 (6th Cir. 1974)). At present, it is unclear how many potential class members exist, where they are located, and whether the potential class members have suffered common injuries. As such, the Plaintiffs are entitled to limited discovery on the facts relevant to the class certification issue.

Accordingly, the Court will address class certification after limited discovery and after the Plaintiffs have properly raised the issue in a motion to certify the class. Still, the Court is sensitive to the potential costs imposed upon the Defendant in continuing to defend this litigation in anticipation of potential class certification. As a result, the parties should engage in

limited and expedited discovery on any facts relevant to the class certification issue and the Plaintiff must move for class certification as soon as possible.

IV. Conclusion

At the pleading stage, the Plaintiffs have provided sufficient information in the complaint to demonstrate Article III standing. Additionally, Plaintiffs' claims for negligence, invasion of privacy based on intrusion upon seclusion, and breach of implied contract may proceed. Still, Plaintiffs have failed to provide sufficient information to demonstrate that they may be entitled to relief on their claims for invasion of privacy based on unreasonable publicity and for breach of fiduciary duty. Lastly, the Court will address the class certification issue upon proper motion from the Plaintiffs and after some limited discovery.

Accordingly, **IT IS ORDERED** as follows:

(1) Allconnect's motion to dismiss and, in the alternative, to strike the class allegations, [DE 5] is **GRANTED IN PART** and **DENIED IN PART**;

(2) Plaintiffs' second cause of action for invasion of privacy is **PARTIALLY DISMISSED** under Rule 12(b)(6) because the Plaintiffs have failed to plead a claim for unreasonable publicity upon which relief may be granted;

(3) Plaintiffs' fourth cause of action for breach of fiduciary duty is **DISMISSED** under Rule 12(b)(6) for failure to state a claim upon which relief may be granted;

(4) Allconnect's motion to dismiss count one, count two under a theory of intrusion upon seclusion, and count three of Plaintiffs' complaint is **DENIED**; and

(5) Allconnect's motion to strike the class allegations from the complaint is **DENIED** at this time.

This the 28th day of March, 2019.

Signed By:
Joseph M. Hood
Senior U.S. District Judge