

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION
CIVIL CASE NO. 1:17-cv-0001-MR-DLH**

**BRYAN CURRY, TERRAN BROOKS,
JERMAINE WILLIS, and BRIAN
HOPPER, on behalf of themselves
and all others similarly situated,**

Plaintiffs,

vs.

SCHLETTER INC.,

Defendant.

**MEMORANDUM OF
DECISION AND ORDER**

THIS MATTER is before the Court on the Defendant's Motion to Dismiss [Doc. 24].

I. PROCEDURAL BACKGROUND

The Plaintiffs, who consist of both former and current employees of the Defendant Schletter Inc., initiated this action on January 3, 2017, asserting claims for negligence, invasion of privacy, breach of implied contract, breach of fiduciary duty, and violations of the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-60, *et seq.* ("NCITPA"), and the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, *et seq.*

(“UDTPA”). [Doc. 1]. After being served with a Summons and a copy of the Complaint, the Defendant filed a Motion to Dismiss. [Doc. 10].

On May 15, 2017, the Plaintiffs filed an Amended Complaint [Doc. 23], thereby rendering the Defendant’s Motion to Dismiss moot. On May 25, 2017, the Defendant filed its second Motion to Dismiss. [Doc. 24]. On June 8, 2017, the Plaintiffs filed their Response in Opposition. [Doc. 26]. On June 15, 2017, the Defendant filed its Reply to the Plaintiffs’ Response. [Doc. 27]. Having been fully briefed, this matter is ripe for disposition.

II. FACTUAL BACKGROUND

Taking the well-pled allegations of the Amended Complaint as true, the following is a summary of the relevant facts.

The Defendant is a part of Schletter Group, a worldwide manufacturer and distributor of solar mountings systems. [Doc. 23 at ¶ 1]. The Defendant’s North American headquarters is in Shelby, North Carolina. [Id.]. The named Plaintiffs are proposed class representatives for a putative class consisting of both current and former employees of the Defendant.¹ [Id. at ¶ 87].

¹ To date, neither the Plaintiffs nor the Defendant have moved for class certification.

As a condition of employment, the Defendant requires that employees entrust it with certain personal information. In its ordinary course of business, the Defendant maintains personal and tax information, including name, address, zip code, date of birth, wage and withholding information, and Social Security number, of its current and former employees (hereinafter, “personal identifying information” or “PII”). The Plaintiffs, as current and former employers, relied on the Defendant to keep this information confidential and securely maintained. [Id. at ¶ 49].

On or about April 19, 2016, the Defendant mailed a form letter to all current and former employees throughout the United States, advising that the employees’ 2015 W-2 tax form information had been sent to an unauthorized third party in response to a W-2 phishing email scam (hereinafter “the Data Disclosure”). [Id. at ¶ 50]. The letter indicated that the Defendant had learned of this incident on or about April 13, 2016, but gave no information as to the actual date when the tax data had been disclosed. [Id. at ¶ 51]. An attachment to the April 19, 2016 letter indicated that the Defendant would be offering credit monitoring and identity theft protection services to those affected for a one-year period. [Id.].

The Defendant sent additional correspondence to its former and current employees on or about April 25, 2016, advising that the Defendant

would extend the identity theft protection and credit monitoring coverage to a period of 24 months. [Id. at ¶ 53].

The Defendant was not without warning of this phishing email scam. On August 27, 2015, the Federal Bureau of Investigation (“FBI”) had issued a report warning of the increasingly common scam, known as Business Email Compromise, in which companies fall victim to phishing emails. Significantly, this report called attention to the significant spike in scams, also referred to as “spoofing,” in which cyber criminals send emails that appear to have initiated from the CEO or other top level executive at the target company. [Id. at ¶ 57]. On February 24, 2016, cybersecurity journalist Brian Krebs warned of the precise scam which snared the Defendant in a blog entitled: “Phishers Spoof CEO, Request W2 Forms.” Krebs warned that cybercriminals were attempting to scam companies by sending false emails, purportedly from the company’s chief executive officer, to individuals in the human resources or accounting department asking for copies of W-2 data for all employees. Krebs even provided an example of such an email that had been sent to another company. [Id. at ¶ 63]. Further, on March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme. [Id. at ¶ 64].

Despite the widespread prevalence of spoofing aimed at obtaining confidential information from employers and despite the warnings of the 2016 tax season W-2 email scam, the Defendant provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure. [Id. at ¶ 65]. Specifically, the Defendant failed to adequately train its employees on even the most basic of cybersecurity protocols, including: (a) how to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate; (b) effective password management and encryption protocols for internal and external emails; (c) avoidance of responding to emails that are suspicious or from unknown sources; (d) locking, encrypting and limiting access to computers and files containing sensitive information; (e) implementing guidelines for maintaining and communicating sensitive data; and (f) protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients. [Id. at ¶ 66].

The Data Disclosure was caused by the Defendant's failure to abide by best practices and industry standards concerning the security of its

computer and payroll processing systems. The Defendant failed to comply with security standards and allowed its employees' PII to be compromised by failing to implement security measures that could have prevented or mitigated the Data Disclosure. The Defendant failed to implement even the most basic of security measures to require encryption of any data file containing PII sent electronically, even within the company. [Id. at ¶ 69].

The Defendant failed to ensure that all personnel in its human resources and accounting departments were made aware of this well-known and well-publicized phishing email scam. [Id. at ¶ 70]. The Defendant also failed to timely disclose the extent of the Data Disclosure, failed to individually notify each of the affected individuals in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Plaintiffs of the nature and extent of the Data Disclosure. By failing to provide adequate and timely notice, the Defendant prevented the Plaintiffs from protecting themselves from the consequences of the Data Disclosure. [Id. at ¶ 71].

The Defendant has not provided compensation to the employees victimized in this Data Disclosure. The Defendant has not offered to provide any assistance or compensation for the costs and burdens, both current and future, associated with the identity theft and fraud resulting from the Data

Disclosure. The Defendant has not offered employees any assistance in dealing with the IRS or state tax agencies. The Defendant has not offered to reimburse employees for the costs, both current and future, incurred as a result of falsely filed tax returns. [Id. at ¶ 82].

To date, the Defendant has offered its employees only two years of identity theft protection through Core ID's ARX-ID Complete service. The Defendant has not offered to reimburse the cost of identity theft protection services purchased by employees before the Defendant gave notice that it would pay for such services. [Id. at ¶ 83]. In any event, the credit monitoring service offered by the Defendant is inadequate to protect the Plaintiffs from the threats they face, particularly in light of the PII stolen. [Id. at ¶ 84]. The enrollment in the credit monitoring service provided by the Defendant has neither prevented the Plaintiffs from experiencing fraudulent activity using their PII nor alerted them that they had fallen victim to identity theft. [Id. at ¶ 85].

As a result of the Defendant's failures to prevent the Data Disclosure, the Plaintiffs allege that they have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. [Id. at ¶ 86].

III. STANDARD OF REVIEW

The central issue for resolving a Rule 12(b)(6) motion is whether the claims state a plausible claim for relief. See Francis v. Giacomelli, 588 F.3d 186, 189 (4th Cir. 2009). In considering Defendant’s motion, the Court accepts the allegations in the Complaint as true and construes them in the light most favorable to Plaintiff. Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 253 (4th Cir. 2009); Giacomelli, 588 F.3d at 190-92. Although the Court accepts well-pled facts as true, it is not required to accept “legal conclusions, elements of a cause of action, and bare assertions devoid of further factual enhancement....” Consumeraffairs.com, 591 F.3d at 255; see also Giacomelli, 588 F.3d at 189.

The claims need not contain “detailed factual allegations,” but must contain sufficient factual allegations to suggest the required elements of a cause of action. Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007); see also Consumeraffairs.com, 591 F.3d at 256. “[A] formulaic recitation of the elements of a cause of action will not do.” Twombly, 550 U.S. at 555. Nor will mere labels and legal conclusions suffice. Id. Rule 8 of the Federal Rules of Civil Procedure “demands more than an unadorned, the defendant-unlawfully-harmed-me accusation.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

The complaint is required to contain “enough facts to state a claim to relief that is plausible on its face.” Twombly, 550 U.S. at 570, 127 S. Ct. at 1974; see also Consumeraffairs.com, 591 F.3d at 255. “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.” Iqbal, 556 U.S. at 678; see also Consumeraffairs.com, 591 F.3d at 255. The mere possibility that a defendant acted unlawfully is not sufficient for a claim to survive a motion to dismiss. Consumeraffairs.com, 591 F.3d at 256; Giacomelli, 588 F.3d at 193. Ultimately, the well-pled factual allegations must move a plaintiff’s claim from possible to plausible. Twombly, 550 U.S. at 570; Consumeraffairs.com, 591 F.3d at 256.

IV. DISCUSSION

A. Negligence and Breach of Implied Contract Claims

The Plaintiffs allege that they were required to provide the Defendant certain PII as a condition of their employment, and that the Defendant had a duty to exercise reasonable care to protect that confidential information. [Doc. 23 at ¶¶ 104-05]. The Defendant’s failure to protect that information, the Plaintiffs contend, gives rise to a claim sounding in negligence, which is pled as their first cause of action. [Id. at ¶¶ 103-22]. Alternatively, in their third cause of action for breach of implied contract, the Plaintiffs characterize

the Defendant's duty to protect their confidential information as arising implicitly from the employment agreement between the Defendant and its employees. [Id. at ¶¶ 133-43].

The Defendant moves to dismiss both claims. With respect to the Plaintiffs' claim for negligence, the Defendant argues that North Carolina's economic loss rules prohibits recovery for economic losses in tort when a contract exists. The Defendant, however, also seeks dismissal of the Plaintiffs' contract claim on the grounds that there was no contract, implied or otherwise, between the parties regarding the safeguarding of PII.

The Court declines to dismiss either claim at this stage. At the heart of both causes of action is the Plaintiffs' assertion that the Defendant, as their employer, had a duty to safeguard and protect the confidential information provided by their employees. Whether such duty arose from the parties' employment contract or from other source remains to be determined from the facts and evidence to be presented. At this juncture, however, the Court is satisfied that the Plaintiffs have adequately stated a cause of action arising from the Defendant's breach of a duty to safeguard their employees' confidential information. Accordingly, the Defendant's motion to dismiss is

denied with respect to the Plaintiffs' claims for negligence and breach of implied contract.²

B. Invasion of Privacy Claim

In their second cause of action, the Plaintiff allege that the Defendant's disclosure of their PII constituted an invasion of their privacy by intrusion. [Doc. 23 at ¶¶ 123-32].

Under North Carolina law, the tort of invasion of privacy by intrusion is defined as the intentional intrusion "physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . [where] the intrusion would be highly offensive to a reasonable person." Miller v. Brooks, 123 N.C. App. 20, 26, 472 S.E.2d 350, 354 (1996) (citation and internal quotation marks omitted), disc. rev. denied, 345 N.C. 344, 483 S.E.2d 172 (1997). "Specific examples of intrusion include physically invading a person's home or other private place, eavesdropping by wiretapping or microphones, peering through windows, persistent

² While this Motion to Dismiss was pending and after it had been fully briefed, the Magistrate Judge directed the parties to brief the issue of whether the Plaintiffs' negligence claim itself states a cause of action notwithstanding the application of the economic loss rule. The Defendant argued in its supplemental briefing that the Plaintiffs' negligence claim could not withstand scrutiny under Rule 12(b)(6) because North Carolina does not establish any such legal duty on the part of an employer to safeguard its employees' private information. Notably, however, the Defendant did not raise this argument in their motion to dismiss. Accordingly, the Court will not address such argument further in the context of the present motion. The parties may revisit the issue of whether such a duty exists under North Carolina law at the summary judgment stage.

telephoning, unauthorized prying into a bank account, and opening personal mail of another.” Burgess v. Busby, 142 N.C. App. 393, 406, 544 S.E.2d 4, 11 (2001).

In Toomer v. Garrett, 155 N.C. App. 462, 574 S.E.2d 76 (2002), disc. rev. denied, 357 N.C. 66, 579 S.E.2d 576 (2003), the plaintiff, a former state employee, alleged that his supervisors intentionally allowed unauthorized individuals access to his state personnel file. The North Carolina Court of Appeals held that the plaintiff had stated a cause of action for invasion of privacy, despite the lack of any physical or sensory intrusion, reasoning that “[t]he unauthorized examination of the contents of one's personnel file, especially where it includes sensitive information such as medical diagnoses and financial information, like the unauthorized opening and perusal of one's mail, would be highly offensive to a reasonable person.” Id. at 480, 574 S.E.2d at 90.

Like the defendants in Toomer, the Defendant in the present case is accused of giving unauthorized persons access to the Plaintiffs’ sensitive information, including their dates of birth, addresses, and Social Security numbers. The Plaintiffs have sufficiently pled allegations to plausibly allege that the Defendant’s actions would be highly offensive to the reasonable person, thus constituting an “intrusion” necessary to sustain a claim for

invasion of privacy under North Carolina law. The Defendant's motion to dismiss the Plaintiffs' second cause of action, therefore, is denied.

C. Breach of Fiduciary Duty Claim

In their fourth cause of action, the Plaintiffs allege that the Defendant was a fiduciary "in matters connected with their employment" and that the Defendant breach its duty of care by failing to adequately protect their PII and W-2 data. [Doc. 23 at ¶¶ 144-48].

Under North Carolina law, "a fiduciary relation is said to exist wherever confidence on one side results in superiority and influence on the other side; where a special confidence is reposed in one who in equity and good conscience is bound to act in good faith and with due regard to the interests of the one reposing the confidence." White v. Consolidated Planning, Inc., 166 N.C. App. 283, 293, 603 S.E.2d 147, 155 (2004), disc. rev. denied, 359 N.C. 286, 610 S.E.2d 717 (2005) (quoting Vail v. Vail, 233 N.C. 109, 114, 63 S.E.2d 202, 206 (1951) (internal quotation marks omitted)). Under North Carolina law, a fiduciary duty generally does not exist between an employer and employee. Dalton v. Camp, 353 N.C. 647, 651, 548 S.E.2d 704, 708 (2001) ("the relation of employer and employee is not one of those regarded as confidential") (citation omitted).

In their Amended Complaint, Plaintiffs simply allege that the Defendant had a fiduciary duty to them by virtue of being their employer. The Plaintiffs fail to make any plausible allegations that their relationship with the Defendant was anything more than a typical employer-employee relationship. Accordingly, the Court concludes that the Plaintiffs have failed to state a claim for breach of fiduciary duty. The Plaintiffs' fourth cause of action, therefore, is dismissed.

D. NCITPA and UDTPA Claims

In their final causes of action, the Plaintiffs allege that the Defendant's actions constitute violations of both the NCITPA and UDTPA. [Doc. 23 at ¶¶ 149-54, 155-66].

While the Amended Complaint is not entirely clear, it appears that the Plaintiffs are alleging two specific violations of the ITPA: § 75-62(a)(1) and § 75-62(a)(6). These provisions provide, in pertinent part, as follows:

[A] business may not do any of the following:

(1) Intentionally communicate or otherwise make available to the general public an individual's social security number.

* * *

(6) Sell, lease, loan, trade, rent, or otherwise intentionally disclose an individual's social security number to a third party without written consent to the disclosure from the individual, when the party making

the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's social security number.

N.C. Gen. Stat. Ann. § 75-62(a)(1), (6). The NCITPA expressly provides that a violation of § 75–62 is also a violation of the UDTPA. N.C. Gen. Stat. § 75-62(d). Therefore, if the Plaintiffs state valid claims under the NCITPA, they also state valid claims under N.C. Gen. Stat. § 75-1.1. Fisher v. Commc'n Workers of Am., No. 08 CVS 3154, 2008 WL 4754850, at *5 (N.C. Super. Oct. 30, 2008).

In order to state a claim under § 75-62(a)(1), a plaintiff must allege three elements: (1) that the defendant is a business; (2) that the defendant communicated or otherwise made available to the general public the plaintiff's Social Security number; and (3) that the defendant acted with intent. Fisher, 2008 WL 4754850, at *5. Here, the Plaintiffs have alleged plausible facts from which a jury reasonably could conclude that the Defendant committed a violation of § 75-62(a)(1) by communicating the Plaintiffs' Social Security numbers to an unknown cybercriminal, thereby rendering the Plaintiffs' otherwise protected and secure information completely *unprotected* and *non-secure*. It is unknown how many cybercriminals were involved in the phishing scam, or whether the Plaintiffs' PII was further disseminated to other cybercriminals. Under these

circumstances, it is not implausible that the Defendant's actions in responding to this phishing scam effectively made the Plaintiffs' Social Security numbers "available to the general public."

The Defendant argues that its actions cannot be considered a violation of § 75-62(a)(1) because it did not "intend to communicate" the Plaintiffs' Social Security numbers to the general public. The Plaintiffs, however, have alleged sufficient facts to support a claim that the Defendant's communication, while solicited under false pretenses, was intentionally made. As the Plaintiffs cogently set out in their brief, this was not a case of a data *breach*, wherein a hacker infiltrated the Defendant's computer systems and stole the Plaintiffs' information, but rather was a case of data *disclosure*, wherein the Defendant intentionally responded to an email request with an unencrypted file containing highly sensitive information regarding its current and former employees. Based on these allegations, the Plaintiffs have sufficiently alleged that the Defendant acted with the requisite intent in communicating this information. See In re Maple, 434 B.R. 363, 372 (Bankr. E.D. Va. 2010) (construing similarly worded Virginia statute to require "only an intent to communicate that which was disclosed" and noting that the statute "does not require the purpose of the communication to be the willful publication of the Social Security number itself").

Turning now to the Plaintiffs' claim under § 75-62(a)(6), the Court finds that the Plaintiffs have sufficiently alleged that the Defendant intentionally disclosed their Social Security numbers to an unauthorized third party and that the Defendant should have known in the exercise of reasonable diligence that the third party lacked a legitimate purpose for obtaining this information.

The Defendant argues that a business does not violate the NCITPA when the alleged activity relates to "the collection, use, or release of a social security number for internal verification or administrative purposes." N.C. Gen. Stat. § 75-62(b)(2). The Defendant's assertion that its action in providing the W-2 information to a cybercriminal constitutes a disclosure for "internal administrative purposes" is an affirmative defense which requires development of the factual record and thus cannot be resolved at the Rule 12(b)(6) stage. See Fisher, 2008 WL 4754850, at *6.

For all of these reasons, the Defendant's motion to dismiss the Plaintiffs' fifth and sixth causes of action is denied.

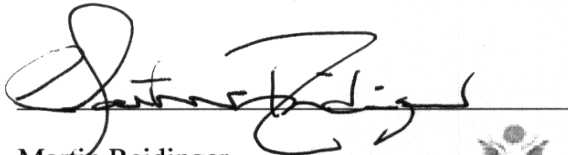
ORDER

IT IS, THEREFORE, ORDERED that the Defendant's Motion to Dismiss [Doc. 24] is **GRANTED IN PART** and **DENIED IN PART**.

Specifically, the Defendant's Motion is **GRANTED** with respect to the Plaintiffs' claim for breach of fiduciary duty, and this claim is **DISMISSED**. In all other respects, the Defendant's Motion is **DENIED**.

IT IS SO ORDERED.

Signed: March 26, 2018


Martin Reidinger
United States District Judge

