United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EVERETT CASTILLO, et al.,

Plaintiffs,

v.

SEAGATE TECHNOLOGY, LLC,

Defendant.

Case No. 16-cv-01958-RS

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

I. INTRODUCTION

In March 2016, someone contacted an employee of defendant Seagate Technology, LLC, requesting 2015 W-2 data for all Seagate employees. Seagate later learned that the request, with which it complied, was part of a phishing scam. After the data leak, some current and former Seagate employees learned that false tax returns had been filed in their names.

Plaintiffs Everett Castillo, Nicholas Dattoma, Freda Lang, Wendy Tran, and Steven Wilk are current and former employees who seek to represent an employee class whose personal information was compromised in the phishing scam. Plaintiff Linda Castillo, the wife of former Seagate employee Everett Castillo, wishes to represent a class of spouses and dependents whose personal information was compromised. Together, plaintiffs advance claims against Seagate for (1) negligence; (2) violations of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 *et seq.*; (3) a declaratory judgment; and (4) breach of implied contract. The breach of contract claim is brought on behalf of the proposed employee class only; the remaining claims

are brought on behalf of all proposed classes. Seagate moves to dismiss all claims with prejudice.

II. BACKGROUND[1]

In March 2016, someone claiming to be Seagate's Chief Executive Officer emailed a handful of Seagate employees to request 2015 Form W-2 information for all Seagate employees. Seagate later discovered this email was part of a phishing scam, prevalent during tax season. Phishers typically send emails to employers hoping to collect sensitive personal information, which they often use subsequently to file false tax returns. Unfortunately, a Seagate employee took the bait and released 2015 W-2 forms for all of the company's current and former employees. These W-2 forms contained personal identifying information — including addresses, salary and benefit information, names, and Social Security numbers — that employees had given Seagate. Armed with this information, the phishers allegedly filed fraudulent tax returns (including, in at least one instance, a joint tax return), in the names of current and former Seagate employees whose information had been disclosed.

A few days after the security breach, Seagate contacted its current employees by email and informed them of the scam. Seagate's Chief Financial Officer told employees the breach was a "mistake . . . caused by human error and lack of vigilance, and could have been prevented." Compl. ¶ 23. Former employees learned the distressing news about a week later by mail. To address employees' concerns, Seagate has offered all current and former employees a two-year subscription to identity theft protection services. It has not offered such services to employees' spouses.

Plaintiffs Everett Castillo, Nicholas Dattoma, Wendy Tran, and Steven Wilk are former Seagate employees whose personal information Seagate compromised. Together with current Seagate employee Freda Lang, they seek to represent a class of current and former Seagate

[1] The facts are drawn from plaintiffs' complaint and are presumed to be true for the purposes of this motion to dismiss.

employees whose personal information was compromised during the attack. Linda Castillo has never worked for Seagate, but her husband, Everett Castillo, gave the company her personal identifying information when he enrolled in a retirement benefits program. Cybercriminals filed a joint tax return using Everett's and Linda's personal identifying information. Ms. Castillo intends to represent a class of non-employees whose information was allegedly compromised in the attack.

After learning of the data breach, each plaintiff discovered that cybercriminals had filed fraudulent tax returns using their personal identifying information. Tran responded by hiring an accountant to help her file her returns properly. Others have spent considerable time and effort to rectify the situation. Dattoma and Wilk purchased additional identity theft protection from Lifelock, and the Castillos are purchasing similar services.

III. LEGAL STANDARD

"A pleading that states a claim for relief 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). "[D]etailed factual allegations are not required," but a complaint must provide sufficient factual allegations to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. v. Twombly*, 550 U.S. 544, 570 (2007)).

Federal Rule of Civil Procedure 12(b)(6) provides a mechanism to test the legal sufficiency of the averments in a complaint. Dismissal is appropriate when the complaint "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). A complaint in whole or in part is subject to dismissal if it lacks a cognizable legal theory or the complaint does not include sufficient facts to support a plausible claim under a cognizable legal theory. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). When evaluating a complaint, the court must accept all its material allegations as true and construe them in the light most favorable to the non-moving party. *Iqbal*, 556 U.S. at 678. "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.* This standard requires "more than a sheer possibility that the defendant

has acted unlawfully." *Id.* "Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Id.* (internal quotation marks omitted). When plaintiffs have failed to state a claim upon which relief can be granted, leave to amend should be granted unless "the complaint could not be saved by any amendment." *Gompper v. VISX, Inc.*, 298 F.3d 893, 898 (9th Cir. 2002).

IV. DISCUSSION

A. Claim 1: Negligence

To state a negligence claim under California law, plaintiffs must plead and prove (1) that Seagate owed them a duty to exercise due care; (2) that Seagate breached that duty; (3) that the breach caused injury; and (4) cognizable injury results. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 959-60 (S.D. Cal. 2012) (citing *Paz v. California*, 22 Cal. 4th 550, 559 (2000)); *see also Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *5 (C.D. Cal. June 15, 2015). Seagate argues all plaintiffs have failed sufficiently to plead duty, causation, or damages, and that Linda Castillo has failed sufficiently to plead the existence of a duty. Seagate also argues that, because plaintiffs seek only economic damages, their negligence claim is barred by California's economic loss doctrine.

1. *Duty, Breach, Causation, and Damages*

a. Duty and Breach

Plaintiffs claim Seagate owed them the duty reasonably to protect their personal identifying information and to inform them reasonably promptly about the phishing attack. Seagate insists plaintiffs fail plausibly to plead facts establishing such duties, particularly to the third-party plaintiffs like Ms. Castillo. "The threshold element of a claim for negligence is the existence of a duty to use due care toward an interest of another that enjoys legal protection against unintentional invasion." *Bily v. Arthur Young & Co.*, 3 Cal. 4th 370, 397 (1992). Whether a duty of care exists is a question of law. *Beacon Residential Cmty. Ass'n v. Skidmore, Owings & Merrill LLP*, 59 Cal. 4th 568, 573 (2014). Of course, plaintiffs may not simply aver that a

defendant owed them a duty. *E.g.*, *Bem v. Stryker Corp.*, No. C 15-2485 MMC, 2015 WL 4573204, at *1 (N.D. Cal. July 29, 2015) ("[Plaintiff's] First Cause of Action, negligence, is deficient, as plaintiff relies solely on conclusory allegations and fails to plead any facts describing the particular defect, the injury sustained, the manner in which [defendant] was negligent, or how any such negligence caused or contributed in any manner to any specified injury."); *Sanchez v. Lending Tree LLC*, No. 10CV1593 JLS, 2010 WL 3983390, at *2 (S.D. Cal. Oct. 12, 2010) (citing *Twombly*, 550 U.S. at 555) (dismissing a negligence claim because the plaintiff averred conclusorily that the defendant breached its duty to protect information).

In California, "each person has a duty to use ordinary care and is liable for injuries caused by his [or her] failure to exercise reasonable care in the circumstances." *Cabral v. Ralphs Grocery Co.*, 51 Cal. 4th 764, 771 (2011) (internal quotation marks omitted) (addressing Cal. Civ. Code § 1714(a)). Here, there are three categories of plaintiffs: current employees, former employees, and employees' spouses and dependents. Thus, each group of plaintiffs must plead facts establishing Seagate owed it a duty. Seagate does not challenge the employee and former-employee plaintiffs' contentions that it owed them a duty to protect their personal identifying information, perhaps because there is no good reason to conclude otherwise. As a condition of employment, employees disclosed the sort of information reasonable people guard closely. They did so with the understanding their employer would guard that information and use it for limited purposes.

Instead, Seagate argues these plaintiffs have inadequately pleaded a breach of duty and have failed to detail how and why Seagate's security measures were unreasonable. While the complaint does not offer specific examples of how Seagate's internal security was deficient, plaintiffs need not plead facts with exactitude to satisfy Rule 8. Plaintiffs imply the problem was inadequate training because one or more Seagate employee responded to a common scam. Accordingly, the employee and former-employee plaintiffs have adequately averred that Seagate breached a duty it owed them.

The more difficult question is whether Seagate owed employees' spouses and dependents a duty reasonably to safeguard their personal identifying information. Plaintiffs rely on the six-

factor test announced in *Rowland v. Christian*, 69 Cal. 2d 108, 111-12 (1968), to support their contention that the scope of Seagate's duty of due care extended to Ms. Castillo and other non-employees. The *Rowland* factors, which determine the reach of a duty, are: (1) "the foreseeability of the harm to the plaintiff"; (2) "the degree of certainty that the plaintiff suffered injury"; (3) "the closeness of the connection between the defendant's conduct and the injury suffered"; (4) "the moral blame attached to the defendant's conduct"; (5) "the policy of preventing future harm"; and (6) "the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach and the availability, cost, and prevalence of insurance for the risk involved." *Rowland*, 69 Cal. 2d at 113.

Five of the six *Rowland* factors suggest Seagate owed its employees' spouses and dependents a duty to safeguard their personal identifying information. Such information is obviously valuable; Social Security numbers unlock various government benefits, employment opportunities, and serve as an important authentication mechanism. Items of such value will always be attractive to unscrupulous people hoping to make quick and easy money, which means attempts to capture such information are likely and foreseeable. That spouses were not Seagate employees does not alter whether cybercriminals would try to collect *any* personal identifying information Seagate had. If Seagate did not take reasonable steps to protect such vital information, and such incautious security resulted in the release of information, then Seagate's conduct would be closely connected with the harm to the plaintiffs, i.e., the release of personal identifying information. In light of the sensitivity of such information, sound public policy would require those who obtain it legally should guard it with care. Moreover, there is likely minimal additional cost of requiring employers to protect the personal identifying information of employees' spouses and dependents with the same degree of care devoted to protecting employee data. Only Seagate's lack of moral culpability counsels against concluding Seagate is duty-bound to protect the personal identifying information of these third parties. Unquestionably, Seagate did not intend or seek to expose their personal identifying information. Nor did Seagate derive any benefits from this data breach. Nonetheless, the *Rowland* factors compel the conclusion Seagate

was duty-bound to take reasonable steps to protect *all* personal identifying information it obtained from its employees, including information pertaining to employees' spouses and dependents.

Even if such duty exists, Seagate further argues the complaint lacks sufficient facts establishing it breached any duty to protect the personal identifying information of the spouse and dependent group. In so arguing, Seagate ignores the averments that hackers managed to file a joint tax return for the Castillos with Ms. Castillo's social security number on the document. That these cybercriminals had access to that sensitive information raises a reasonable inference that Seagate had and released such sensitive information to the phishers. If Ms. Castillo proves, as she alleges, Seagate requested from its employees the personal identifying information of spouses and dependents to enroll them in health and retirement benefits, then she can show Seagate had a duty to those people to protect that critical information.

Plaintiffs aver Seagate breached a second duty — the duty to inform them of the security breach in a reasonably timely manner so they could take steps to monitor for unauthorized use of their personal identifying information. For the reasons discussed above, when Seagate asked for and obtained the personal identifying information of its employees and their spouses, it assumed a duty to protect that information — a duty that included prompt notice of security breaches.

b. Causation

To state a claim for negligence, plaintiffs must plead facts that plausibly connect the alleged breach of duty to the harm plaintiffs suffered. *In re Sony*, 996 F. Supp. 2d at 964. After learning about the phishing attack, each named plaintiff discovered that tax returns had been filed using his or her personal identifying information. This raises a reasonable inference the person who filed the fraudulent tax return obtained plaintiffs' personal identifying information from the Seagate phisher — information obtained allegedly due to Seagate's lax security measures. Tran's case, however, is different. She concedes her personal identifying information had been compromised during a previous, unrelated data breach. Compl. ¶ 28. She has thus not provided sufficient information to conclude her 2015 federal tax return was filed as a result of the Seagate data breach. An equally strong inference, on the basis of these facts, is that the fraudulent 2015

tax return was traceable to the fact that her personal information already circulated among certain cyber scoundrels. To create a reasonable inference the Seagate data breach caused the 2015 filing, Tran should plead more particular facts connecting the two events, such as the temporal relationship between the breach and the false filing, or the similarities between the false filing in her name and the filings in the names of other Seagate personnel.

All plaintiffs but Tran have adequately pleaded that Seagate's alleged negligence caused their harm. The remaining question is whether those alleged harms are cognizable damages supporting a negligence claim.

c. Damages

Negligence claims also require plaintiffs to connect the defendant's allegedly negligent conduct to a cognizable, nonspeculative harm. *In re Sony*, 903 F. Supp. 2d at 962 (citing *Aas*, 24 Cal. 4th at 646). "[S]peculative harm or the mere threat of future harm is insufficient to constitute actual loss." *Corona*, 2015 WL 3916744, at *3 (citing *Jordache Enters., Inc. v. Brobeck, Pheger & Harrison*, 18 Cal. 4th 739 (1998)).

Plaintiffs claim Seagate's negligence caused the following injuries: (1) out-of-pocket costs related to the false tax returns filed; (2) increased costs associated with preparing and filing tax returns; (3) out-of-pocket costs connected with procuring additional identity protection and restoration services; (4) out-of-pocket costs associated with credit repair in the event of a future identity theft; and (5) lost productivity and enjoyment as a result of monitoring use of personal identifying information. Compl. ¶ 53. Only some of the plaintiffs have actually incurred out-of-pocket expenses so far. Tran hired an accountant to help her navigate the process of refiling tax returns. *Id.* ¶ 26. Dattona and Wilk bought a subscription to LifeLock, an identity-protection service, because they wanted greater protection than that offered by Seagate. *Id.* ¶¶ 31, 33. In contrast, the Castillos are merely considering purchasing such services, *id.* ¶ 30, and Lang has not incurred any out-of-pocket expenses, *id.* ¶ 32. Those who have incurred such out-of-pocket expenses have pleaded cognizable injuries, whereas those who claim only that they may incur expenses in the future have not. *See Corona*, 2015 WL 3916744, at *4 (concluding the increased

risk of future harm and lost time are not cognizable injuries in a data-breach case, as opposed to expenses incurred to pay for identity-theft protection). Accordingly, only Tran, Dattona, and Wilk have pleaded cognizable injuries; Lang and the Castillos have not.

No plaintiffs, meanwhile, have stated a cognizable injury that resulted from Seagate's alleged failure to provide adequate and timely notice of the breach. They have not, for example, pleaded any facts suggesting timelier or more adequate notice would have prevented the filing of fraudulent tax returns. *See id.* at *5. Instead, plaintiffs rely upon *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1171 (D. Minn. 2014), where the district court concluded plaintiffs had pleaded a cognizable injury flowing from Target's alleged failure to provide timely notice of the breach. Yet, *In re Target* is distinguishable because the hackers had made unlawful purchases using plaintiffs' credit card information, which caused plaintiffs to incur fraudulent fees, to lose access to their bank accounts, and to pay new card fees. *Id.* at 1159. Here, none of the plaintiffs avers such similar economic harm, and therefore they have not successfully traced Seagate's alleged breach of its duty promptly to provide notice of the phishing attack to any cognizable injury.

2. *The Economic Loss Doctrine*

Not only must plaintiffs plead cognizable, nonspeculative harm, but under California law, plaintiffs asserting negligence claims ordinarily may not recover purely economic damages unconnected to physical injury or property damage. *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 315 F. App'x 603, 605 (9th Cir. 2008)); *In re Sony*, 903 F. Supp. 2d at 961 (citing *Aas v. Superior Court*, 24 Cal. 4th 627 (2000)).[2] Economic losses include damages for inadequate value,

[2] Plaintiffs insist the economic loss doctrine only applies to claims of product defectiveness, but they do not identify any authorities so holding. Indeed, the Ninth Circuit has spoken to the contrary. *See Kalitta*, 315 F. App'x at 605 (citations omitted) ("Generally speaking, in actions for negligence, liability is limited to damages for physical injuries and recovery of economic loss is not allowed. . . . In the absence of (1) personal injury, (2) physical damage to property, (3) a 'special relationship' existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed."); *Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 874 (9th Cir. 2007) ("the economic loss doctrine has not been confined to product liability cases").

costs of repair, loss of expected proceeds, loss of use, loss of goodwill, and damages paid to third parties. *Id.* at n.15. At its core, the economic loss doctrine is about the scope of a defendant's duty to a plaintiff and whether the plaintiff's economic losses are entitled to legal protection. *See J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 803 (1979) (describing the economic loss doctrine).

Plaintiffs contend Seagate breached two separate, but related duties: (1) the duty to protect their personal identifying information; and (2) the duty to inform them promptly and adequately after discovering the data breach. Not one of the plaintiffs suffered personal injury as a result of the data breach, and the damages they seek to recover are economic in nature. Thus, the economic loss doctrine bars plaintiffs' negligence claim unless they had a "special relationship" with Seagate. *In re Sony*, 903 F. Supp. 2d at 961. California courts consider six criteria to determine whether such a relationship exists:

> (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.

J'Aire, 24 Cal. 3d at 804.

Some of the factors suggest Seagate and plaintiffs had a "special relationship." Seagate required employees to provide personal identifying information as a condition of employment. In addition, to obtain health insurance coverage and to enroll in retirement plans, employees had to disclose the personal identifying information of their spouses and children. These benefit programs were designed to affect the employees and their families. *See Corona*, 2015 WL 3916744, at *5 (holding that where plaintiffs gave their personal identifying information to receive compensation and employment benefits, there could be "no doubt" the transaction was "intended to affect" the plaintiffs). Plaintiffs also allege a close connection between Seagate's conduct (releasing personal identifying information) and the harm they suffered (identity theft). Once the personal identifying information was released to the wrong individuals, the filing of false tax returns is a natural consequence flowing from the careless release of information. Moreover, the

need to protect such sensitive information from similar attacks in the future is great.

Nonetheless, plaintiffs cannot show the harm they suffered was foreseeable or that Seagate is morally culpable in this ordeal. Plaintiffs insist this data breach was foreseeable because an Internet security research firm wrote an article about the sort of phishing scam to which Seagate fell prey. In *Corona*, the district court concluded a data breach and resulting injury to former employees were foreseeable because the defendant had been the victim of similar phishing attacks in the past and was aware of similar breaches at other companies. *See* 2015 WL 3916744, at *5. In contrast, plaintiffs here have not provided any information about whether Seagate was aware of this article or knew about similar data breaches. Plaintiffs also have not provided enough information to permit an inference that Seagate should have been on the lookout for fraudulent requests for W-2 information. Absent such averments, plaintiffs have failed adequately to plead that Seagate's actions were immoral. *See Mega RV Corp. v. HWH Corp.*, 225 Cal. App. 4th 1318, 1342 (2014), *as modified on denial of reh'g* (May 20, 2014), *review denied* (July 9, 2014) (finding no moral blame absent evidence of reckless or purposeful behavior).

Accordingly, plaintiffs have failed to plead facts establishing their special relationship with Seagate, and the economic loss doctrine bars their claim. The claim is therefore dismissed with leave to amend. Although this complaint does not plead a viable claim for negligence, plaintiffs may be able to state a claim by offering facts establishing Seagate was aware of similar phishing scams or even that they failed to alert those with access to employees' personal identifying information about how to protect against phishing attacks.

B. Claim 2: UCL

California's Unfair Competition Law proscribes all unlawful, unfair, or fraudulent business acts or practices. Cal. Bus. & Prof. Code § 17200 *et seq.* "Each prong of the UCL is a separate and distinct theory of liability." *Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Under the unlawful prong, a plaintiff must allege the defendant violated another law. Under the unfair prong, a plaintiff must allege facts to establish "the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers" or tether the UCL

claim "to some specific constitutional, statutory, or regulatory provisions." *Hodsdon v. Mars, Inc.*, 162 F. Supp. 3d 1016 (N.D. Cal. 2016) (internal quotation marks omitted). Plaintiffs do not allege Seagate's conduct violates the fraudulent prong of the UCL.[3]

1. *The Unlawful Prong*

The UCL's unlawful prong allows plaintiffs to "borrow" other laws and make claims independently actionable under the UCL. *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). Plaintiffs argue Seagate violated the UCL's prohibition of unlawful activities through its alleged negligence and alleged violation of California's Customer Records Act ("CRA"), Cal. Civ. Code §1798.80, *et seq.*[4] Barring success in amending the negligence claim, *see supra* Part IV.A., plaintiffs cannot depend on it as the "unlawful" predicate for UCL purposes.

Plaintiffs' argument that Seagate violated the CRA in connection with the data breach, on the other hand, may support a claim of unlawful practices under California's UCL. Although the CRA is primarily concerned with the protection of customer data, *see, e.g.*, *id.* § 1798.81 ("A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records[.]"), and provides remedies only for customers harmed by its violation, *id.* § 1798.84, its plain language nonetheless operates to protect some non-customer information. Specifically, the statute expresses "the intent of the Legislature to ensure that personal information about California residents is protected" and requires "reasonable security procedures and practices appropriate" to

[3] Because plaintiffs do not raise a fraud claim, no heightened pleading standard applies. *See* Fed. R. Civ. P. 9(b) ("In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."). Plaintiffs' claims under the "unlawful" and "unfair" prongs of the UCL are held only to the ordinary pleading requirements of Rule 8.

[4] Even if the underlying law contains no private right of action, it can still serve as the predicate for a UCL claim — unless the plaintiff attempts to use the UCL to "plead around an absolute bar to relief." *Yanting Zhang v. Superior Court*, 57 Cal. 4th 364, 368-69 (2013) (citation and internal quotation marks omitted). Seagate does not argue that the CRA or the law of negligence erects an absolute bar to relief for plaintiffs, and neither the law of negligence nor the text of the CRA supports such an argument. Although Seagate argues that the CRA offers no protection to plaintiffs because they are not Seagate customers, this argument fails for the reasons that follow.

protect personal information that businesses "own, license, or maintain." *Id.* § 1798.81.5(a)-(b). Although the statute specifies, for the section covering "[s]ecurity procedures and practices with respect to personal information about California residents," that "the terms 'own' and 'license' *include* personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates," the terms are not *limited* to customer information. *Id.* (emphasis added). Moreover, the relevant sections of the statute place no limit on the scope of maintained information that falls under its protection. *See id* §§ 1798.81.5, 1798.82.

In addition to mandating security procedures, the statute requires that "a person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.* § 1798.82(b). Together, these security and reporting provisions plainly require the protection by businesses of non-customer personal information that they maintain.

Plaintiffs allege that Seagate's inadequate security practices failed to protect personal information it maintained from falling into unauthorized hands, and that Seagate did not immediately notify them of the phishing attack upon learning of it — that Seagate waited a few days to tell employees, then a few more to tell former employees. Plaintiffs have adequately pleaded unlawful practices under the UCL through violation of the CRA.

2. *The Unfair Prong*

What activities constitute "unfair" business practices under the UCL is an issue currently in flux. *See Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012). California courts have used two different definitions of an "unfair" business practice for consumer cases. First, many courts have found a business practice "unfair" when it "is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App. 4th 861, 886-87 (1999) (internal quotation marks

omitted). This approach requires courts to "examine the practice's 'impact on its alleged victim, balanced against the reasons, justifications and motives of the alleged wrongdoer.'" *Davis*, 691 F.3d at 1169 (quoting *S. Bay Chevrolet*, 72 Cal. App. 4th at 887). The California Supreme Court has criticized this approach, however, as "too amorphous" to provide meaningful "guidance to courts and businesses." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 185 (1999).

"The second test — the public policy test — requires that the UCL claim be tethered to some specific constitutional, statutory, or regulatory provisions." *McVicar v. Goodman Glob., Inc.*, 1 F. Supp. 3d 1044, 1054 (C.D. Cal. 2014) (citations and internal quotation marks omitted). Absent guidance from the California courts about the proper definition of an "unfair" business practice, federal courts have applied both tests. *See Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 736 (9th Cir. 2007) (citations omitted) ("The remaining options, then, are to apply *Cel-Tech* directly to this case and require that the unfairness be tied to a 'legislatively declared' policy, or to adhere to the former balancing test under *South Bay*. These options, however, are not mutually exclusive.").

Under either formulation, the plaintiffs have adequately pleaded a claim. The "public policy" test clearly supports a claim because the plaintiffs have pleaded a violation of an underlying law — California's CRA. *See supra* Part IV.B.2. The balancing test also supports a claim here, because Seagate cannot offer a compelling reason or justification for its allegedly weak security protocol and mishandling of information that would outweigh the effect on plaintiffs of having false tax returns filed in their names.

3. *The Availability of Restitution or Injunctive Relief*

Although plaintiffs have adequately pleaded violations of the unlawful and unfair prong of California's UCL, they nonetheless fail sufficiently to plead entitlement to restitution or injunctive relief, the only forms of relief available under the UCL. *See* Cal. Bus. & Prof. Code § 17203. Restitution is unavailable because plaintiffs do not allege that Seagate obtained from them any money or other financial benefit. *See In re Sony*, 996 F. Supp. 2d at 970. Plaintiffs also fail

sufficiently to allege a threat of impending future harm that would entitle them to injunctive relief. *See Rahman v. Mott's LLP*, No. CV 13-3482 SI, 2014 WL 5282106, at *5 (N.D. Cal. Oct. 15, 2014), *reconsideration denied*, No. 13-CV-03482-SI, 2014 WL 6815779 (N.D. Cal. Dec. 3, 2014) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983)) (additional citation omitted) ("To have standing to obtain injunctive relief, a plaintiff must allege that a 'real or immediate threat' exists that he will be wronged again."). Plaintiffs' argument that they have suffered an injury as a result of having false tax returns filed in their names may be relevant to the question of whether they have any Article III standing in this case, but it does not relate to any potential future harm that would support standing to seek injunctive relief. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, (2000) ("a plaintiff must demonstrate standing separately for each form of relief sought"). Moreover, plaintiffs' attempt to argue that they face an "increased risk of future identity theft," is speculative and thus insufficient to show a cognizable threat of future harm. *See In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (citing *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 (2013)) (additional citations omitted) ("The Court therefore finds that the increased threat of identity theft and fraud stemming from the Zappos's security breach does not constitute an injury-in-fact sufficient to confer standing. . . . The possibility that . . . alleged harm could transpire in the as-of-yet undetermined future relegates Plaintiffs' injuries to the realm of speculation. . . . The degree of Plaintiffs' speculation is heightened further by the fact that the future harm is based entirely on the decisions or capabilities of an independent, and unidentified, actor."). Because plaintiffs have not adequately pleaded standing to seek restitution or injunctive relief, their UCL claim is dismissed with leave to amend.

C. Claim 3: Declaratory Judgment

Pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201-02, plaintiffs seek a declaration that Seagate's protection of personal identifying information is deficient and that, to comply with its duty to protect such information, it must implement nine practices. *See* Compl. ¶ 71. Congress did not create new substantive rights by passing the Declaratory Judgment Act, but instead expanded the remedies available to plaintiffs with otherwise viable claims for relief.

Skelly Oil Co. v. Phillips Petrol. Co., 339 U.S. 667, 671 (1950); *Harris Cty. Texas v. MERSCORP Inc.*, 791 F.3d 545, 552 (5th Cir. 2015); *Wishnev v. Nw. Mut. Life Ins. Co.*, No. 15-CV-03797-EMC, 2016 WL 493221, at *17 (N.D. Cal. Feb. 9, 2016). To qualify for the relief the Act created, plaintiffs must present a "definite and concrete," "real and substantial" "case of actual controversy" that touches upon the "legal relations of parties having adverse interests." *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007) (internal quotation marks omitted). Moreover, the declaration may not be "an opinion advising what the law would be upon a hypothetical state of facts." *Id.* (internal quotation marks omitted).

Plaintiffs' complaint appears to seek declaratory relief pursuant to only their negligence and UCL claims. These claims have not been adequately pleaded. *See supra* Parts IV.A-B. Absent viable substantive claims, plaintiffs cannot seek declaratory relief, and therefore this claim is dismissed with leave to amend.

D. Claim 4: Breach of Implied Contract

The proposed employee class claims that Seagate committed breach of implied contract by failing adequately to safeguard employee personal information. "An implied contract is one, the existence and terms of which are manifested by conduct." Cal. Civ. Code § 1621. To plead breach of an implied contract, a plaintiff must allege: "(1) the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to plaintiff." *Reichert v. Gen. Ins. Co. of Am.*, 68 Cal. 2d 822, 830 (1968) (citations omitted). Seagate argues that plaintiffs have failed sufficiently to allege the existence of a contract and breach.

1. *The Existence of a Contract*

"An implied-in-fact contract requires proof of the same elements necessary to evidence an express contract: mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter." *Corona*, 2015 WL 3916744, at *6 (citation and internal quotation marks omitted). An implied contract requires that both parties agree to its terms and have a "meeting of the minds," *Blaustein v. Burton*, 9 Cal. App. 3d 161, 179 (1970), but the creation of an implied contract can be manifested by conduct rather than words, *see T & M Solar & Air Conditioning,*

Inc. v. Lennox Int'l Inc., 83 F. Supp. 3d 855, 872 (N.D. Cal. 2015). The existence of an implied contract is an issue of fact. *See Acri v. Varian Assocs., Inc.*, 121 F.3d 714 (9th Cir. 1997) (remanding for trial the issue of whether "an implied contract to terminate only for good cause" existed).

Seagate first argues plaintiffs have alleged no conduct evincing mutual assent or offer and acceptance. The upshot of the averments in the plaintiffs' complaint however, is quite clear: The employees provided their personal information for tax purposes and to receive employment and benefits, with the understanding that Seagate, while it held the information, would take adequate measures to protect it. Seagate received the personal information so that it could employ the plaintiffs, and provide them with employment and benefits. While Seagate made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently. *See In re Target*, 66 F. Supp. 3d at 1176 (holding that the plaintiffs had sufficiently pleaded "an implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to safeguard Plaintiffs' personal and financial information.").

Seagate also makes the related argument that plaintiffs fail to specify the scope of protection to which it allegedly assented. It cites no authority, however, for the proposition that plaintiffs must plead the scope of the contract term with great specificity. Instead, it points to *In re Anthem, Inc. Data Breach Litig.*, which dismissed an implied breach of contract claim supported by only one line in the plaintiffs' original complaint: "[b]y demanding and accepting Plaintiffs' and Statewide Class Members' [personal identifying information], Anthem and Anthem Affiliates entered into implied contracts with Plaintiffs and Statewide Class Members." 162 F. Supp. 3d 953 (N.D. Cal. 2016). Plaintiffs here have alleged more than their *Anthem* counterparts; they have alleged an implied contract term that Seagate would take "adequate measures" and make "reasonable efforts" to "properly safeguard[]" its employees personal identifying information.

Defendants have identified no authority requiring more specificity, and it is difficult to imagine how plaintiffs, who are not assumed to be experts in the field of data protection, could have formed highly particular expectations about the measures that would be taken to protect their information. Moreover, to require a specifically pleaded scope of data protection for an *implied* breach of contract claim would operate to preclude such a claim between all but the most sophisticated and familiar parties. Even if the party sharing his or her data had very specific expectations about the measures that would be taken to protect it, it would be exceedingly difficult to show the recipient assented to those precise protective measures. Plaintiffs' claim is a far more realistic reflection of the mutual agreement that occurs in most data-sharing transactions: When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected.

Finally, Seagate argues that plaintiffs' pleading alleges an implied contract in which Seagate would protect personal information of only active employees. This simply rehashes the argument that the scope of protection was ill-defined. Plaintiffs allege that Seagate implicitly agreed to take "adequate measures" and make "reasonable efforts" to "properly safeguard[]" the personal information of employees. This is adequate to plead a claim of implied breach of contract for former employees. A factfinder can ultimately determine whether an implied contract to protect adequately plaintiffs' information existed, and whether such a contract for adequate protection required protection beyond an employment term.

2. *Breach of Contract*[5]

Plaintiffs aver that Seagate breached the implied contract term to take "adequate measures" and make "reasonable efforts" to "properly safeguard[]" the personal information of its employees by "fail[ing] to safeguard and protect" that information. Plaintiffs' complaint quotes an email from Seagate's chief financial officer admitting the data theft "was caused by human error and lack of vigilance, and could have been prevented." Compl. ¶ 23. This is more than sufficient to allege that Seagate breached a duty to safeguard plaintiffs' personal identifying information adequately.

V. CONCLUSION

With regards to the negligence, UCL, and declaratory judgment claims, defendant's motion to dismiss is granted with leave to amend. Any amended complaint shall be filed within 20 days of this order. Defendant's motion to dismiss plaintiffs' breach of implied contract claim is denied.

IT IS SO ORDERED.

Dated: September 14, 2016

RICHARD SEEBORG
United States District Judge

[5] The parties' papers create some confusion about whether plaintiffs' have pleaded breach of implied contract, breach of implied covenant, or both. Although the complaint uses the word covenant — "Indeed, a material term of this contract is a covenant by Seagate that it will take reasonable efforts to safeguard Employees' PII" — it also uses synonyms like "promise" and "obligation" to refer to Seagate's alleged responsibility to protect plaintiffs' information. Moreover, the claim itself is explicitly styled as a breach of contract claim, and the covenant language seems simply to refer to a *term* of the alleged implied contract. Whatever its linguistic shortcomings, the complaint plainly attempts to plead breach of contract, and not breach of covenant. Thus, it is not necessary to apply the high standard that attaches to a claim for breach of implied covenant of good faith and fair dealing: "failure or refusal to discharge contractual responsibilities, prompted not by an honest mistake, bad judgment or negligence but rather by a conscious and deliberate act, which unfairly frustrates the agreed common purposes and disappoints the reasonable expectations of the other party thereby depriving that party of the benefits of the agreement." *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011).