UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: MICHAELS STORES PIN PAD LITIGATION	)	11 C 3350
This Document Relates to All Actions	)	

MEMORANDUM OPINION

CHARLES P. KOCORAS, District Judge:

This case comes before the Court on the motion of Defendant Michaels Stores, Inc. ("Michaels") to dismiss the Consolidated Amended Class Action Complaint (the "Complaint") pursuant to Federal Rule of Civil Procedure 12(b)(6). For the reasons stated below, the motion is granted in part and denied in part.

BACKGROUND[1]

Michaels is a specialty arts and crafts retailer. Like many other retailers, Michaels uses PIN pads to process customers' debit and credit card payments. To make a debit or credit card purchase through a PIN pad, a cardholder swipes his or her card through the PIN pad and, if necessary, inputs a personal identification number ("PIN"). A properly operating PIN pad encrypts the cardholder's PIN, temporarily stores the encrypted PIN, and transmits the information to a transaction manager, card company, or bank for verification.

[1] For purposes of the motion to dismiss, we accept the allegations of the Complaint as true. *Warth v. Seldin*, 422 U.S. 490, 501 (1975).

"Skimming" is the unauthorized capture of debit and/or credit card data by unauthorized persons, often referred to as "skimmers." Skimmers use the information in a number of illegal ways, including selling the information or creating a fraudulent duplicate card. One method skimmers use to obtain debit and credit card information from retail stores is referred to as "PIN pad swapping." Using this method, skimmers remove a legitimate PIN pad from a merchant's store and replace it with a modified PIN pad that captures the debit and credit card information and the customer's PIN. The swapped PIN pad then stores the data for later physical retrieval by the skimmers or wirelessly transmits the data to the skimmers.

Michaels accepts customer payments for purchases through credit and debit cards issued by members of the payment card industry ("PCI"), such as Visa USA ("Visa"). Some card issuers, like Visa, contractually obligate merchants, like Michaels, to comply with various PIN pad security standards that protect customer financial information as a condition to processing transactions through the card issuer. In 2005, Visa issued a global mandate ("Visa's Global Mandate") that required merchants to discontinue the use of PIN pad terminals that do not meet the Triple Data Encryption Standard by July 1, 2010. Visa also required merchants to implement certain operating regulations to protect the security of cardholder information (the "PCI PIN Security Requirements"). Among numerous other requirements, the PCI PIN Security Requirements direct

merchants to ensure that a legitimate device has not been substituted with a counterfeit device. In 2006, Visa and other PCI members established the Security Standards Council ("PCI SSC"), which has developed stringent standards for PIN pad terminals. Additionally, PCI SSC, PIN pad manufacturers, and credit card processors have developed and implemented a series of best practices for merchants to prevent or identify instances of skimming, including PIN pad swapping.

On May 4, 2011, Michaels reported that PIN pad tampering may have occurred in its Chicago area stores. Michaels later revealed that between February 8, 2011, and May 6, 2011, skimmers placed approximately ninety tampered PIN pads in eighty Michaels stores across twenty states. At the time of the security breaches, Michaels was not in compliance with Visa's Global Mandate or the PCI PIN Security Requirements.

On July 8, 2011, Plaintiffs Mary Allen, Kelly M. Maucieri, Brandi Ramundo, and Adrianna Sierra (collectively, "Plaintiffs") filed the Complaint against Michaels individually and on behalf of all consumers whose financial information was stolen from Michaels. Plaintiffs allege that Michaels failed to adequately protect their financial information and failed to promptly and properly notify consumers of the security breach. Plaintiffs further allege that the data breach resulted in unauthorized withdrawals from their bank accounts and/or bank fees. Plaintiffs assert claims under the Stored Communications Act, 18 U.S.C. § 2702, and the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1, and for negligence,

negligence *per se*, and breach of implied contract. Michaels now moves to dismiss the Complaint.

LEGAL STANDARD

A pleading 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). Rule 8 does not require detailed factual allegations, but requires more than legal conclusions or a formulaic recitation of the elements of a cause of action. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). To survive a motion to dismiss, the complaint must contain sufficient facts to state a claim for relief that is plausible on its face. *Id.* at 570. In ruling on a motion to dismiss, a court accepts the well-pleaded allegations in the complaint as true, construes the allegations of the complaint in the light most favorable to the plaintiff, and draws all reasonable inferences in favor of the plaintiff. *Hentosh v. Herman M. Finch Univ. of Health Scis./The Chi. Med. Sch.*, 167 F.3d 1170, 1173 (7th Cir. 1999).

DISCUSSION

I. Stored Communications Act[2]

The Stored Communications Act ("SCA") states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic

[2] Because a plain reading of the statute yields support for both parties' positions, the Court finds that the statute is ambiguous and refers to the legislative intent to aid its interpretation. *See United States v. Hudspeth*, 42 F.3d 1015, 1022 (7th Cir. 1994).

storage by that service." 18 U.S.C. § 2702(a)(1). The SCA further states that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service." 18 U.S.C. § 2702(a)(2). Michaels argues that the SCA does not apply because it does not provide electronic communication services or remote computing services.

A. Electronic Communication Services

The first issue is whether Michaels provides electronic communication services under the SCA. An "electronic communication service" is "any service which provides to users the ability to send or receive wire or electronic communications." 18 U.S.C. §§ 2510(15), 2711(1). According to the SCA's legislative history, telephone companies and electronic mail companies provide electronic communication services. S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3558. Since the enactment of the SCA, courts have consistently acknowledged that internet service providers, e-mail service providers, and telecommunication companies also provide electronic communication services under the SCA. *Steinbach v. Village of Forest Park*, 2009 WL 2605283, at *5 (N.D. Ill. Aug. 25, 2009) (finding that the Village of Forest Park did not provide electronic communication services because it provided the e-mail address and not the e-mail or internet service); *United States v. Weaver*, 636 F. Supp. 2d 769, 769-70 (C.D. Ill. 2009) (noting that Microsoft, the internet and e-mail service provider,

provided electronic communication services and remote computing services); *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 901-04 (N.D. Ill. 2006) (assuming that AT&T, a telecommunications company providing telephone and internet services, provides electronic communication services); *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (concluding that defendant who did not provide internet services did not provide electronic communication services by maintaining an internal e-mail system).

When determining whether an entity provides electronic communication services, courts consider whether the entity is in the business of providing electronic communication services. *See, e.g., In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005) (explaining that JetBlue's maintenance of a website did not convert it into a provider of electronic communication services; rather, JetBlue is a provider of air travel services and a consumer of electronic communication services); *Dyer v. Northwest Airlines Corps.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("businesses offering their traditional products and services online through a website are not providing an 'electronic communication service'"); *Andersen Consulting*, 991 F. Supp. at 1043 (explaining that the defendant, a supplier to the petroleum and gas processing industries, was not in the business of providing electronic communication services even though it maintained an internal e-mail system). Ultimately, the provider of an electronic communication service is the provider of the underlying service which

transports the data, such as an internet service provider or a telecommunications company whose cables and phone lines carry internet traffic, and not the provider of a product or service which facilitates the data transport.

Here, Plaintiffs allege that Michaels provides electronic communication services because Michaels, through its PIN pads, enables consumers to pay with credit and debit cards and send or receive electronic communications concerning their account data and PINs to transaction managers, card companies, or banks. Significantly, Plaintiffs do not allege that Michaels provides the internet or phone service through which the PIN pad communicates. This insufficiency is fatal to Plaintiffs' claim that Michaels provides electronic communication services under the SCA. Further, Michaels, a retailer of specialty arts and crafts, is not in the business of providing electronic communication services, even though it maintains PIN pads, a necessary tool for almost any retailer today. *See, e.g. Andersen Consulting*, 991 F. Supp. at 1043 (explaining that defendant's internal e-mail system is a necessary tool for most businesses). This Court shares the concern of the *Andersen* court, as Plaintiffs' interpretation of the statute would convert every single retailer using a PIN pad into a provider of electronic communication services under the SCA. Finally, the alleged data breach has nothing to do with the provision of electronic communication services because the skimmers obtained the information from the mere swipe of the card on the PIN pad and not when the

underlying service transmitted the information to a third party for approval. For these reasons, Michaels does not provide electronic communication services under the SCA.

B. Remote Computing Services

Although the Court finds that Michaels does not provide electronic communication services, the SCA nevertheless applies if Michaels provides remote computing services. A "remote computing service" is "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). Remote computing services exist to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564. Some businesses use remote computing services to process data remotely on someone else's equipment rather than in-house. *Id.*

Plaintiffs allege that Michaels provides remote computing services because the PIN pads electronically store and remotely process consumers' payment information. While Plaintiffs artfully tailor their allegations to the language of the SCA, Michaels does not provide remote computing services as contemplated by the statute. In particular, Plaintiffs' allegations fail to demonstrate that Michaels, a retailer of specialty arts and crafts, provides any off-site computer storage or computer processing services. Accordingly, Michaels does not provide remote computing services under the SCA.

Because Michaels provides neither electronic communication services nor remote computing services, the Court dismisses Plaintiffs' SCA claim. The Court thus need not address Michaels' remaining arguments.

II. Illinois Consumer Fraud and Deceptive Business Practices Act

To state a claim under the Illinois Consumer Fraud Act ("ICFA"), a plaintiff must allege that (1) the defendant engaged in a deceptive or unfair practice, (2) the defendant intended for the plaintiff to rely on the deception, (3) the deception occurred in the course of conduct involving trade or commerce, (4) plaintiff sustained actual damages, and (5) such damages were proximately caused by the defendant's deception. *Martis v. Pekin Mem'l Hosp. Inc.*, 917 N.E.2d 598, 603 (Ill. App. Ct. 2009). Michaels argues that Plaintiffs fail to state a claim under the ICFA because the allegations do not demonstrate that Michaels engaged in a deceptive or unfair practice or that Plaintiffs suffered actual damage. Michaels also argues that Plaintiffs cannot establish an ICFA claim based on a violation of the Illinois Personal Information Protection Act. The Court addresses each argument below.

A. Deceptive Practice

Michaels argues that Plaintiffs' allegations fail to demonstrate that Michaels engaged in a deceptive practice. The Illinois Supreme Court has declared that a plaintiff cannot maintain an action under the ICFA for a deceptive practice absent some communication from the defendant, either a communication containing a deceptive

misrepresentation or a deceptive omission. *De Bouse v. Bayer AG*, 922 N.E.2d 309, 316 (Ill. 2009) (holding that plaintiff had no ICFA claim where plaintiff had seen no advertisements for the drug and had no independent knowledge of the drug or its effects). For instance, in *Ciszewski v. Denny's Corp.*, the plaintiff sued a restaurant for knowingly failing to disclose the excessive sodium content of its meals. 2010 WL 1418582, at *2 (N.D. Ill. Apr. 7, 2010). The *Ciszewski* court dismissed plaintiff's ICFA claim because plaintiff could not identify a communication from the defendant containing the deceptive omission. *Id.* at *3.

This case is strikingly similar to *Ciszewski*. Like the allegedly deceptive omission in *Ciszewski*, Plaintiffs allege that they were deceived by Michaels' failure to disclose that it had not implemented adequate security measures. Also, as in *Ciszewski*, Plaintiffs identify no communication by Michaels which contained this allegedly deceptive omission. The Court thus follows the holding in *Ciszewski*, and finds that Plaintiffs fail to allege that Michaels engaged in a deceptive practice. Accordingly, the Court declines to address Michaels' additional argument that Plaintiffs' deception claim improperly relies on the same factual foundation as Plaintiffs' implied contract claim.

B. Unfair Practice

Michaels also argues that Plaintiffs' allegations cannot show that Michaels engaged in an unfair practice. To determine whether a practice is unfair under the ICFA, the court considers whether the practice offends public policy, whether it is

immoral, unethical, oppressive, or unscrupulous, and whether it causes substantial injury to consumers. *Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 961 (Ill. 2002). A plaintiff does not need to satisfy all three criteria to support a finding of unfairness. *Id.* A practice may be unfair because of the degree to which it meets one of the criteria or because to a lesser extent it meets all three. *Id.* Further, when interpreting the ICFA, the court should consider interpretations of the Federal Trade Commission ("FTC") and the federal courts relating to Section 5(a) of the Federal Trade Commission Act. 815 Ill. Comp. Stat. 505/2.

The First Circuit, in a case also involving the hacking of customer credit and debit card information due to a company's failure to follow security protocols, found that the plaintiffs stated a claim for unfair practices under Massachusetts law. *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 495-96 (1st Cir. 2009). Specifically, the First Circuit stated that, based on the FTC criteria, a court could find that the company's lack of security measures constitutes an unfair practice because such conduct is systematically reckless, "aggravated by [a] failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers." *Id.* at 496.

Here, Plaintiffs allege that Michaels failed to comply with Visa's Global Mandate, requiring the use of tamper-resistant PIN pads, and with the PCI Pin Security Requirements. Plaintiffs further allege that Michaels failed to promptly notify

consumers of the security breach. As determined by the First Circuit in *TJX*, such conduct could constitute an unfair practice because it causes substantial injury to consumers.

Michaels contends that Plaintiffs' allegations are deficient because they fail to identify which PCI Pin Security Requirements Michaels violated and how Michaels did not adhere to the industry's best practices. However, Plaintiffs allege that the PCI PIN Security Requirements and the industry's best practices obligated Michaels to implement procedures and practices to ensure that a legitimate device had not been substituted with a counterfeit device. Since Plaintiffs allege that the skimmers did, in fact, substitute legitimate devices with counterfeit devices, Plaintiffs' allegations show that Michaels ignored its obligation to implement procedures and practices preventing the criminal conduct. Plaintiffs thus sufficiently allege that Michaels engaged in an unfair practice under the ICFA.

C. Actual Damage

Michaels further argues that Plaintiffs fail to allege they suffered actual damage under the ICFA. Only a person who suffers actual damage may bring an action under the ICFA. 815 Ill. Comp. Stat. 505/10a(a). The plaintiff must allege a purely economic injury, measurable by the plaintiff's loss. *Morris v. Harvey Cycle & Camper, Inc.*, 911 N.E.2d 1049, 1053 (Ill. App. Ct. 2009); *see Mulligan v. QVC, Inc.*, 888 N.E.2d 1190,

1197-98 (Ill. App. Ct. 2008) ("If the plaintiff is not materially harmed by the defendant's conduct, however flagrant it may have been, there may be no recovery.").

Plaintiffs maintain that they suffered actual damages in many forms. First, Plaintiffs argue that they suffered actual damages because of the costs associated with the increased risk of identity theft, including the present and future costs of credit monitoring services. However, under the ICFA, a plaintiff does not suffer actual damage simply because of the increased risk of future identity theft or because the plaintiff purchased credit monitoring services. *Cooney v. Chi. Public Sch.*, 943 N.E.2d 23, 31 (Ill. App. Ct. 2010). Plaintiffs, relying on *Rowe v. UniCare Life & Health Ins. Co.*, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010), assert that Illinois law allows recovery of damages incurred to mitigate the risk of future harm. Plaintiffs' reliance on *Rowe* is misplaced because the court confirmed that the cost of credit monitoring services and the increased risk of future harm are not present injuries under the ICFA, despite the fact that a plaintiff can recover damages for the increased risk of future harm. *Rowe*, 2010 WL 86391, at *5-7; *see Williams v. Manchester*, 888 N.E.2d 1, 13 (Ill. 2008) ("as a matter of law, an increased risk of future harm is an *element of damages* that can be recovered for a present injury–it is not the injury itself"). *Rowe* correctly draws a distinction between the injury requirement under the ICFA and the damages that a plaintiff may recover. Moreover, Plaintiffs' interpretation would unfairly allow individuals to create standing under the ICFA. To illustrate, imagine two similarly

situated individuals impacted by Michaels' allegedly unfair practice, but only one individual purchased credit monitoring services. According to Plaintiffs' reasoning, only the individual who purchased the credit monitoring services has standing to sue under the ICFA while the other does not. This unfair result supports the position that individuals cannot create standing by voluntarily incurring costs in response to a defendant's act. Accordingly, Plaintiffs cannot rely on the increased risk of identity theft or the costs of credit monitoring services to satisfy the ICFA's injury requirement.

Second, Plaintiffs argue that they suffered monetary losses from unauthorized bank account withdrawals and/or related bank fees charged to their accounts. Michaels contends that such allegations are insufficient because Plaintiffs failed to allege that they paid the charges or were not reimbursed for the charges. Michaels is correct that Plaintiffs suffered no actual injury under the ICFA if Plaintiffs were reimbursed for all unauthorized withdrawals and bank fees and, thus, suffered no out-of-pocket losses. *See, e.g., Clark v. Experian Information Solutions, Inc.*, 2006 WL 2224049, at *3 (N.D. Ill. Aug. 2, 2006) (granting summary judgment on plaintiff's ICFA claim because plaintiff suffered no actual damages since she either received a full refund or a full refund was available to her upon request). However, because Plaintiffs allege that they lost money, the Court can reasonably infer that Plaintiffs were not reimbursed for all

fees and charges. Accordingly, Plaintiffs sufficiently allege that they suffered actual injuries when they lost money from unauthorized withdrawals and/or bank fees.[3]

D. Illinois Personal Information Protection Act

Michaels argues that Plaintiffs cannot establish an ICFA claim based on the Illinois Personal Information Protection Act ("PIPA"). A violation of PIPA constitutes an unlawful practice under the ICFA. 815 Ill. Comp. Stat. 530/20. PIPA requires data collectors who own personal information concerning an Illinois resident to notify the resident of a data breach "in the most expedient time possible and without unreasonable delay . . . ." 815 Ill. Comp. Stat. 530/10.

Plaintiffs allege that Michaels violated PIPA by failing to timely notify affected customers of the nature and extent of the security breach. Michaels responds that it timely notified consumers of the security breach and properly provided consumers with substitute notice. However, a disputed issue of facts exists regarding when Michaels first learned of the data breach and, thus, whether Michaels timely notified consumers. Michaels cannot overcome this disputed issue by relying on self-serving statements from its website that it learned of the security breach the same week it notified consumers. Further, the Complaint does not show that Michaels had a right to provide

[3] For this reason, Plaintiffs properly allege a compensable injury for all of their claims and the Court need not address Plaintiffs' remaining contention that they suffered actual injury because Michaels damaged Plaintiffs' property rights in their personal information.

substitute notice under PIPA. Accordingly, Plaintiffs state a plausible claim under the ICFA based on Michaels' alleged violation of PIPA.

III. Negligence & Negligence *Per Se*

To state a claim for negligence, a plaintiff must allege that the defendant owed a duty to the plaintiff, the defendant breached that duty, and the breach caused injury to the plaintiff. *Cooney*, 943 N.E.2d at 27 (finding that defendants had no statutory or common law duty to safeguard plaintiffs' personal information).

Michaels argues that Plaintiffs' negligence claims fail for two reasons. First, Michaels contends that the intervening acts of criminals broke the causal chain. Generally, a defendant will not be held liable for negligence if an intervening criminal act causes the plaintiff's injury. *Rowe v. State Bank of Lombard*, 531 N.E.2d 1358, 1368 (Ill. 1988). However, an exception exists where the defendant's acts or omissions create a condition conducive to a foreseeable intervening criminal act. *Id.* In such cases, the causal chain is not broken by a reasonably foreseeable intervening act. *Id.*

Here, Plaintiffs allege that Michaels failed to comply with various PIN pad security requirements, which were specifically designed to minimize the risk of exposing their financial information to third parties. Because the security measures could have prevented the criminal acts committed by the skimmers, Michaels failure to implement such measures created a condition conducive to a foreseeable intervening

criminal act. Accordingly, the skimmers' reasonably foreseeable intervening criminal act did not sever the causal chain.

Second, Michaels asserts that Illinois' economic loss rule bars Plaintiffs' negligence claims. The economic loss rule bars a plaintiff from recovering for purely economic losses under a tort theory of negligence. *Moorman Mfg. Co. v. Nat'l Tank Co.*, 435 N.E. 2d 443, 453 (Ill. 1982). The rationale underlying this doctrine is that tort law affords the proper remedy for loss arising from personal injury or damages to one's property, whereas contract law and the Uniform Commercial Code provide the appropriate remedy for economic loss stemming from diminished commercial expectations without related injury to person or property. *In re Ill. Bell Switching Station Litig.*, 641 N.E.2d 440, 444 (Ill. 1994).

Illinois law recognizes three exceptions to the economic loss rule: (1) where plaintiff sustains personal injury or property damage resulting from a sudden or dangerous occurrence; (2) where plaintiff's damages were proximately caused by defendant's intentional, false representation; and (3) where plaintiff's damages were proximately caused by the negligent misrepresentation of a defendant in the business of supplying information for the guidance of others in business transactions. *Moorman*, 435 N.E.2d at 450-52.

Because the economic loss rule and its exceptions have been applied inconsistently by federal courts in Illinois, the Court examines the evolution of the

doctrine in the Illinois Supreme Court. The Illinois Supreme Court first applied the economic loss rule in the context of a product liability action. In *Moorman*, where a defective product only damaged itself and did not cause any separate property damage, the court held that the plaintiff could not recover for the cost of repairs and loss of use under the tort theories of strict liability or negligence. 435 N.E.2d at 445, 448, 451. The court reasoned that "the essence of a product liability tort case is not that the plaintiff failed to receive the quality of product he expected, but that the plaintiff has been exposed, through a hazardous product, to an unreasonable risk of injury to his person or property." *Id.* at 448. The court further explained that "contract law, which protects expectation interests, provides the proper standard when a qualitative defect is involved." *Id.* Thus, where only the defective product is damaged, a plaintiff cannot recover in tort for economic losses caused by the qualitative defect and stemming from disappointed expectations about the product's performance. *Id.* at 450.

Just a few years after *Moorman*, the Illinois Supreme Court extended the doctrine and held that the economic loss rule bars a claim that a defendant negligently performed services. *Anderson Elec. v. Ledbetter Erection Corp.*, 503 N.E.2d 246, 249 (Ill. 1986) (holding economic loss rule applied where plaintiff claimed that defendant negligently performed the inspection and approval of plaintiff's work). The court also held that "[a] plaintiff seeking to recover purely economic losses due to defeated expectations of a

commercial bargain cannot recover in tort, regardless of the plaintiff's inability to recover under an action in contract." *Anderson Elec.*, 503 N.E.2d at 249.

Over the next few years, the Illinois Supreme Court dealt with the applicability of the economic loss rule to claims of professional malpractice against a defendant providing services. The court held that the economic loss rule did not apply to a plaintiff asserting a professional malpractice claim against an attorney or an accounting firm. *Collins v. Reynard*, 607 N.E.2d 1185, 1187 (Ill. 1992) (attorney); *Congregation of the Passion, Holy Cross Province v. Touche Ross & Co.*, 636 N.E.2d 503, 515 (Ill. 1994) (accounting firm). The court in *Congregation of the Passion* set forth a test for determining when the economic loss rule applies to professional malpractice claims. *Congregation of the Passion*, 636 N.E.2d at 514-15. The court held that the doctrine does not apply to the service industry, where the ultimate result of the defendant's work is intangible, if the defendant allegedly breached a duty owed to the plaintiff independent of any contract. *Id.* at 514-15. Regarding an accountant, the court found that an accountant's duty to observe reasonable professional competence exists independently of any contract because accountants "have long been held to be members of a skilled profession, and liable for their negligent failure to observe reasonable professional competence." *Id.* at 515. Accordingly, the economic loss doctrine did not bar plaintiff's professional malpractice claim against the accounting firm. *Id.*

Following the analysis set forth in *Congregation of the Passion*, the Illinois Supreme Court later found that the economic loss doctrine bars recovery in tort against engineers for purely economic losses because the ultimate result of an engineer's work is a tangible product. *Fireman's Fund Ins. Co. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1201-02 (Ill. 1997).[4] More specifically, in *Fireman's Fund*, the defendant engineer was hired to create plans for a water supply system. *Id.* at 1198. The Illinois Supreme Court held that the ultimate result of the engineer's work was a tangible product, the water supply system, and that the engineer's plans and drawings were incidental to that tangible product. *Id.* at 1201-02.

Here, Plaintiffs do not dispute the fact that they seek to recover in tort solely for economic losses. The economic loss rule bars Plaintiffs' negligence and negligence *per se* claims unless Plaintiffs satisfy an exception to the rule. Plaintiffs do not argue that they satisfy any of the three exceptions set forth in *Moorman*. Rather, Plaintiffs argue that the economic loss rule does not apply because Michaels breached a duty owed to Plaintiffs independent of any contractual obligation or warranty. However, the exception to which Plaintiffs refer, as announced in *Congregation of the Passion*, only applies to professional malpractice claims where the ultimate result of the defendant's

[4] It is unclear whether the independent duty exception is a fourth exception to the economic loss rule or part of the negligent misrepresentation exception. *Compare Congregation of the Passion*, 636 N.E.2d at 515 (creating an exception to the economic loss rule apart from the negligent misrepresentation exception), *with Fireman's Fund*, 679 N.E.2d at 1201-02 -+(viewing the analysis in *Congregation of the Passion* under the negligent misrepresentation exception).

work is intangible. *See Congregation of the Passion*, 636 N.E.2d at 514-15; *see also Fireman's Fund*, 679 N.E.2d 1201-02. Based on the allegations in the complaint, Plaintiffs' negligence claims do not relate to professional malpractice and the ultimate result of the transaction was the sale of products to Plaintiffs, not the provision of intangible services.[5] Accordingly, the exception articulated in *Congregation of the Passion* does not apply to this case.

Plaintiffs also attempt to avoid the economic loss rule by arguing that it does not apply to Michaels' willful conduct. Aside from the intentional misrepresentation exception identified in *Moorman*, no such exception exists. Indeed, the Illinois Supreme Court barred an action for purely economic losses allegedly due to the defendant's "negligent or willful" conduct. *In re Ill. Bell Switching Station Litig.*, 641 N.E.2d at 441-42, 444 (holding that the customers of defendant telephone company could not recover economic damages they incurred from the loss of telephone service after defendant's telephone switching station caught fire due to defendant's negligent

[5] Plaintiffs cite several non-binding cases where courts have interpreted *Congregation of the Passion* as simply holding that the economic loss rule does not apply if the defendant breached a duty owed to the plaintiff independent of any contract. *See, e.g., Choi v .Chase Manhattan Mortg. Co.*, 63 F. Supp. 2d 874, 883-85 (N.D. Ill. 1999) (finding the economic loss rule inapplicable where defendants had a duty to manage plaintiff's escrow account and the accompanying tax obligations with professional competence and due care); *see also Serfecz v. Jewel Food Stores, Inc.*, 1998 WL 142427, at *3-4 (N.D. Ill. 1998) (recognizing that *Congregation of the Passion* created an exception for professional malpractice, yet extending the exception where the tenant owed the landlord a common law duty not to commit waste). Even if this Court accepted such a broad interpretation of *Congregation of the Passion*, Plaintiffs identify no historical or common law duty owed by merchants to consumers.

or willful failure to take adequate fire-prevention measures). Plaintiffs thus fail to allege an exception to the economic loss rule.

Notably, other courts dealing with data breach cases have also held that the economic loss doctrine bars the plaintiff's tort claim because the plaintiff has not suffered personal injury or property damage. *See, e.g., In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d at 498-99 (applying Massachusetts law and affirming dismissal of bank's negligence claim based on economic loss doctrine because bank did not suffer property damage); *see also Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175-77 (3d Cir. 2008) (applying Pennsylvania law and affirming dismissal of bank's negligence claim based on economic loss doctrine because bank did not suffer property damage); *see also Cumis Ins. Society, Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 46-47 (Mass. 2009) (applying Massachusetts law and affirming dismissal of negligence claim of credit unions who issued the compromised credit cards because the credit unions cannot sue in tort for purely economic losses). This Court follows suit.

For these reasons, the Court dismisses Plaintiffs' negligence and negligence *per se* claims.

IV. Breach of Implied Contract

An implied in fact contract is created by the parties' conduct and contains all of the elements of an express contract - offer, acceptance, and consideration - as well as

a meeting of the minds. *Brody v. Finch Univ. of Health Scis./The Chi. Medical Sch.*, 698 N.E.2d 257, 265 (Ill. App. Ct. 1998).

Michaels argues that Plaintiffs' implied contract claim fails because Plaintiffs have not alleged facts showing the existence of an implied contract. Specifically, Michaels, without relying on any particular case, contends that the facts alleged do not demonstrate that the parties intended to create a contract governing how Michaels would safeguard Plaintiffs' financial information and when Michaels would notify consumers of a security breach.

The First Circuit recently evaluated an implied contract claim in a similar case involving the unauthorized use of plaintiffs' credit and debit card data after hackers breached the defendant's electronic payment system. *Anderson v. Hannaford Bros.*, 2011 WL 5007175, at *1 (1st Cir. Oct. 20, 2011). The First Circuit affirmed the district court's finding that a jury could reasonably find an implied contract between the defendant and its customers that defendant would take reasonable measures to protect the customers' financial information. *Id.* at *5. The court elaborated that "[w]hen a customer uses a credit card in a commercial transaction, she intends to provide the data to the merchant only . . . and does not expect – and certainly does not intend — the merchant to allow unauthorized third parties to access that data." *Id.* "A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract." *Id.* The Court finds such reasoning persuasive

and holds that the allegations demonstrate the existence of an implicit contractual relationship between Plaintiffs and Michaels, which obligated Michaels to take reasonable measures to protect Plaintiffs' financial information and notify Plaintiffs of a security breach within a reasonable amount of time.[6] Accordingly, the Court denies Michaels' motion to dismiss Plaintiffs' claim for breach of an implied contract.

CONCLUSION

For the foregoing reasons, the Court grants in part and denies in part Michaels' motion to dismiss and dismisses Plaintiffs' SCA claim and negligence claims.

Charles P. Kocoras
United States District Judge

Dated: November 23, 2011

[6] Michaels broadly contends that "[c]ourts routinely reject consumer breach of implied contract claims in data exposure cases," and cites *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007) and *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775 (W.D. Mich. 2006). However, in both *Pisciotta* and *Hendricks*, the courts found that the plaintiffs' breach of contract claims failed because the cost of credit monitoring services and the increased risk of future identity theft were not existing, compensable injuries where no actual misuse of consumer data had occurred. *Pisciotta*, 499 F.3d at 632, 635, 639; *Hendricks*, 444 F. Supp. 2d at 777, 780. However, as discussed above, the Plaintiffs in this case allege that criminals have misused their financial information and caused Plaintiffs to lose money from unauthorized withdrawals and/or related bank fees.