

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

<b>BRANDON WORIX, individually and on behalf of all others similarly situated,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>vs.</b>	)	<b>Case No. 11 C 8088</b>
	)	
<b>MEDASSETS, INC.</b>	)	
	)	
<b>Defendant.</b>	)	

**MEMORANDUM OPINION AND ORDER**

MATTHEW F. KENNELLY, District Judge:

Brandon Worix, on behalf of himself and a putative class of similarly situated individuals, has sued MedAssets, Inc. for its alleged failure to implement adequate safeguards to protect his personal information and to notify him properly when a computer hard drive containing that information was stolen. Worix asserts claims under the Stored Communications Act (SCA), 18 U.S.C. § 2702, the Illinois Consumer Fraud Act (ICFA), 815 ILCS 505/2, and Illinois common law. He filed the case in state court, and MedAssets removed it to federal court, citing the Class Action Fairness Act, 28 U.S.C. § 1332(d)(3), as well as federal question jurisdiction under 28 U.S.C. § 1331.

MedAssets has moved to dismiss all of Worix’s claims pursuant to Federal Rule of Civil Procedure 12(b)(6). For the reasons stated below, the Court grants the motion.

**Background**

The Court takes the following facts from Worix’s complaint and accepts them as true for purposes of the motion to dismiss. *Virnich v. Vorwald*, 664 F.3d 206, 212 (7th

Cir. 2011).

MedAssets describes itself as a “financial improvement partner for health care providers.” Compl. ¶ 6. It handles personal and confidential information involving thousands of individuals, including patients of the Cook County Health & Hospitals System (CCHHS). Worix is one of these patients.

On June 24, 2011, an unknown person stole a computer hard drive from a MedAssets employee’s car. Worix alleges that the hard drive contained information including the names, birthdays, and social security numbers of over 82,000 patients, including 32,000 CCHHS patients. The information was neither encrypted nor password protected.

Worix later received a letter dated August 19, 2011. The letter, written on CCHHS letterhead and signed by officials of both CCHHS and MedAssets, stated that the hard drive had been stolen. The letter also stated that the hard drive contained “names, encounter numbers and administrative information” but not “addresses, birth date[s], and social security number[s].” It also stated that the information was not password-protected or encrypted. The letter offered an apology as well as a call-in number if the recipient wanted more information, but no other form of relief. *Id.* Ex. A.

Worix claims that “MedAssets failed to adequately secure patients’ personal health records” and that “[t]he security breach and corresponding data breach arising therefrom was caused by MedAssets’ knowing violation of its government-mandated obligations to abide by best practices and industry standards concerning the security of medical information.” *Id.* ¶¶ 9-10. He claims that MedAssets then “sent a deficient notification of the breach, inadequately describing exactly what information was

accessible and failing to mention what remedial steps CCHHS patients – or better yet, MedAssets – could take to ensure CCHHS patients’ identities were not stolen.” *Id.* ¶ 11.

Worix asserts a claim under the SCA on behalf of himself and a putative class of “[a]ll persons residing in the United States whose personal and/or medical information was contained on the stolen hard drive in June 2011.” *Id.* ¶ 14. He argues that as a result of MedAssets’ alleged violations of the SCA, he and the other class members have “suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring and/or identity theft protection services to protect against additional identity theft.” *Id.* ¶ 32. He also asserts claims for negligence and negligence *per se*, contending that he and the class members “suffered theft of sensitive, non-public, information, and . . . incurred the additional costs associated with increased risk of identity theft, all of which have ascertainable value to be proven at trial.” *Id.* ¶ 40. Finally, Worix asserts a claim under the ICFA on behalf of himself and a putative subclass of Illinois residents. He argues that MedAssets violated the statute by failing to take proper security precautions and provide immediate notice of the breach to affected customers.

### **Discussion**

“Dismissal for failure to state a claim under Rule 12(b)(6) is proper ‘when the allegations in a complaint, however true, could not raise a claim of entitlement to relief.’” *Virnich*, 664 F.3d at 212 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 558 (2007)). “In reviewing a plaintiff’s claim, the court must construe all of the plaintiff’s factual allegations as true, and must draw all reasonable inferences in the plaintiff’s favor. However, legal conclusions and conclusory allegations merely reciting the

elements of the claim are not entitled to this presumption.” *Id.* (citing *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1951 (2009)). “To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Iqbal*, 129 S. Ct. at 1949 (internal quotation marks and citation omitted).

**A. Stored Communications Act**

In count one of his complaint, Worix seeks relief under 18 U.S.C. § 2702(a)(1), which provides 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 storage by that service.” Alternatively, he seeks relief under 18 U.S.C. § 2702(a)(2), which provides 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.”

MedAssets argues for dismissal of count one on three grounds: the company is neither an “electronic communication service” nor a “remote computing service” provider; it does not provide its services “to the public”; and it did not “knowingly divulge” any protected information. Worix does not dispute that he must establish all three of these elements. Because the Court concludes that Worix cannot show that MedAssets knowingly divulged his information, it need not reach the other two arguments.

MedAssets argues that its alleged failure to take steps that would protect the information in the event of the hard drive’s theft, even if true, did not constitute “knowingly divulg[ing]” information under the SCA. MedAssets relies primarily on *Muskovich v. Crowell*, No. 3-95-CV-20007, 1996 WL 707008 (S.D. Iowa Aug. 30, 1996).

In that case, an MCI employee harassed a customer whose phone number he retrieved from company records. The customer alleged that MCI had violated the SCA “by failing to implement adequate security procedures to prevent unauthorized access to the content of electronic information under its control” and that the company “knew or should have known that by failing to safeguard against unauthorized access to electronic communications, MCI knowingly divulged” private information. *Id.* at \*3. The court granted summary judgment for MCI. Noting that neither the statute nor other case law defined “knowingly” for purposes of the SCA, the court based its conclusion primarily on the following legislative history:

The term knowingly means that the defendant was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness of or a firm belief about the substantial certainty of the result. The conduct in question is the act of disclosure. The result is that the contents have been provided to another person or entity. The circumstances involved are that the person involved provides electronic communication services to the public and that the contents relate to a wire or electronic communication. Knowledge as to a circumstance includes willful blindness. The concept of “knowingly” does not include, however, “reckless” or “negligent” conduct.

H.R. Rep. No. 647, 99th Cong., 2nd Sess. at 64 (1986).

The court in *Muskovich* conceded that MCI could have known that its alleged failure to implement safeguards would increase the possibility that an employee would abuse its records in this manner but concluded that this did not amount to “knowingly divulg[ing]” information within the meaning of the statute. The court concluded that an “[a]wareness of a ‘possibility’ does not rise to the level of awareness of a ‘substantial certainty’ required for liability under the [SCA].” *Id.* at \*5.

MedAssets also points to *Freedman v. America Online, Inc.*, 329 F. Supp. 2d

745, 749 (E.D. Va. 2004), in which the court understood the legislative history of the SCA to indicate that a “plaintiff must show that defendant was aware, or possessed a firm belief, that his act would result in the disclosure of the . . . information to another person or entity.” The court found “no doubt” that the defendant in that case had “knowingly divulged information” because the defendant “did not disclose the information inadvertently” and was “aware that by faxing the [allegedly confidential] subscriber information . . . this information would certainly be disclosed.” *Id.*

Neither *Muskovich* nor *Freedman* is binding on this Court. And legislative history is not always a clear guide to the meaning of a statutory term. But *Muskovich*, *Freedman*, and the legislative history all read the statutory requirement of “knowing” conduct consistently with that term’s commonly-accepted legal meaning in the criminal-law context (the SCA is a criminal statute). Specifically, the common meaning of knowing conduct includes willful blindness, but not recklessness or negligence.

The doctrine of willful blindness is well established in criminal law. Many criminal statutes require proof that a defendant acted knowingly or willfully, and courts applying the doctrine of willful blindness hold that defendants cannot escape the reach of these statutes by deliberately shielding themselves from clear evidence of critical facts that are strongly suggested by the circumstances. The traditional rationale for this doctrine is that defendants who behave in this manner are just as culpable as those who have actual knowledge.

*Global-Tech Appliances, Inc. v. SEB S.A.*, 131 S. Ct. 2060, 2068-69 (2011). “[A] willfully blind defendant is one who takes deliberate actions to avoid confirming a high probability of wrongdoing and who almost can be said to have actually known the critical facts.” *Id.* at 2070-71. “By contrast, a reckless defendant is one who merely knows of a substantial and unjustified risk of such wrongdoing, and a negligent defendant is one

who should have known of a similar risk but, in fact, did not.” *Id.* at 2071 (citations omitted).

Worix argues that he has alleged that MedAssets deliberately failed to encrypt or password-protect the data and that “[b]y failing to take commercially reasonable steps to safeguard sensitive patient data, MedAssets has knowingly divulged” the information. Compl. ¶ 31. The first of these allegations is beside the point, and the latter is insufficient. The SCA requires proof that the defendant “knowingly *divulge[d]*” covered information, not merely that the defendant knowingly failed to protect the data. 18 U.S.C. § 2702(a)(1) & (2). And the failure to take reasonable steps to safeguard data does not, without more, amount to divulging that data knowingly or with willful blindness.

Worix argues further that his allegations are different from those in *Muskovich* because “MedAssets had – at the very least – a firm belief that the ‘requisite circumstances’ were present for a theft and subsequent data breach to occur.” Pl.’s Resp. at 8. He contends that this renders the theft of the hard drive “distinguishable from the unforeseeable security breach” in *Muskovich*. *Id.* Worix fails to explain, however, how an unknown actor’s theft of data from unsecured equipment is more foreseeable than a theft by an employee known to have access to the data. Moreover, Worix offers no legal support for his contention that MedAssets’ alleged knowledge of the circumstances that allowed for the theft rendered it “substantially certain” that the theft would occur. Failing to password-protect or encrypt data, though perhaps risky, does not make its receipt by a third party virtually certain, unlike sending a fax, which is what occurred in *Freedman*.

The Court concludes that in the present circumstances, Worix’s conclusory

allegation that MedAssets knowingly divulged data fails to meet *Iqbal*'s plausibility requirement. Worix's allegations might support a contention that MedAssets acted recklessly or negligently, but that does not amount to knowingly divulging the data. See *Global-Tech*, 131 S. Ct. at 2071 (contrasting a defendant who has knowledge under the doctrine of willful blindness with "a reckless defendant . . . who merely knows of a substantial and unjustified risk of wrongdoing").

For these reasons, the Court dismisses Worix's SCA claim.

## **B. Negligence**

MedAssets contends that the Court should dismiss Worix's claims for negligence and negligence *per se* because he has not alleged facts that establish that MedAssets owed him a duty; the theft of the hard drive was an unforeseeable intervening event that "cuts off" causation; and he has failed to allege that he has actually suffered an injury. The Court agrees that Worix has not alleged that he suffered an injury under Illinois negligence law.

Illinois law requires "legally cognizable *present* injury or damage" to sustain a negligence claim. *Yu v. Int'l Bus. Machs. Corp.*, 314 Ill. App. 3d 892, 897, 732 N.E.2d 1173, 1177 (2000) (emphasis added). MedAssets argues that Worix has not alleged that he has actually suffered the loss of any money or property but rather has alleged only that he is subject to an increased risk of identity theft and that he must now pay for credit monitoring. Worix does not dispute this characterization of his allegations, only the allegations' legal effect.

A "federal court sitting in diversity [is] charged with predicting how [the state supreme court] would decide if presented with the identical issue." *Dumas v. Infinity*



*Broad. Corp.*, 416 F.3d 671, 680 n.11 (7th Cir. 2005). The Illinois Supreme Court has held that “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.” *Williams v. Manchester*, 228 Ill. 2d 404, 425, 888 N.E.2d 1, 13 (2008) (emphasis in original).

Applying *Williams*, another judge in this district has held that a plaintiff whose personal data had been compromised “may collect damages based on the increased risk of future harm he incurred, but only if he can show that he suffered from some present injury beyond the mere exposure of his information to the public.” *Rowe v. UniCare Life and Health Ins. Co.*, No. 09 C 2286, 2010 WL 86391, at \*6 (N.D. Ill. Jan. 5, 2010). The judge in *Rowe* denied the defendants’ motion to dismiss because the plaintiff had alleged that he suffered emotional distress, which, if proven, could constitute the required present injury. Unlike the plaintiff in *Rowe*, Worix has alleged no present injury.

No Illinois decision of which the Court is aware has analyzed this precise issue in the negligence context. “In the absence of any authority from the relevant state courts, [a federal court] shall examine the reasoning of courts in other jurisdictions addressing the same issue and applying their own law for whatever guidance about the probable direction of state law they may provide.” *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 635 (7th Cir. 2007). In *Pisciotta*, the Seventh Circuit conducted such an examination to determine whether Indiana negligence law supported allegations similar to Worix’s against a bank whose website was breached by a hacker. After finding that no Indiana case established that credit monitoring costs constituted present injury, the court found that analogous cases from other jurisdictions all “rel[ied] on the same basic premise:

Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.” *Id.* at 639.

Many other decisions have echoed this reasoning. The Oregon Supreme Court recently held that allegations that did not include “actual identity theft or financial harm, other than credit monitoring and similar mitigation costs” did not allege sufficient “present injury” under the state’s “well-established negligence requirements.” *Paul v. Providence Health System-Oregon*, \_\_\_ P.3d \_\_\_, No. S059131, 2012 WL 604183, at \*6 (Or. Feb. 24, 2012) (internal quotation marks and citation omitted). The District of Columbia Court of Appeals has ruled similarly, citing a significant number of analogous decisions from other jurisdictions. *Randolph v. ING Life Ins. and Annuity Co.*, 973 A.2d 702, 708 (D.C. 2009) (collecting cases). In particular, the court cited *Shafran v. Harley-Davidson, Inc.*, No. 07 C 1365, 2008 WL 763177, at \*3 (S.D.N.Y. Mar. 24, 2008), in which the court noted that “[c]ourts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law [of negligence] is prepared to remedy.”

Like the Seventh Circuit in *Pisciotta*, numerous federal courts applying state law have come to the same conclusion. *See, e.g., Krottner v. Starbucks Corp.*, 406 Fed. Appx. 129, 131-32 (9th Cir. 2010); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1054-55 (E.D. Mo. 2009); *Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc.*, No. 08 C 1568, 2009 WL 799760, at \*3 (E.D. La. Mar. 24, 2009); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 281-82 (S.D.N.Y. 2008); *Hendricks v. DSW ShowWarehouse, Inc.*, 444 F. Supp. 2d 776, 783 (W.D. Mich. 2006); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006). In

so holding, courts have sometimes noted that plaintiffs asserting these claims “have pointed to no case decided anywhere in the country where a court allowed a negligence claim to survive absent an allegation of actual identity theft.” *McLoughlin v. People’s United Bank, Inc.*, No. 3:08 C 944, 2009 WL 2843269, at \*8 (D. Conn. Aug. 31, 2009); see also *Hammond v. Bank of New York Mellon Corp.*, No. 08 C 6060, 2010 WL 2643307, at \*1 (S.D.N.Y. June 25, 2010) (collecting cases).

Worix cites several cases, including *Pisciotta*, holding that allegations like his are sufficient to establish injury-in-fact for purposes of Article III standing. See *Pisciotta*, 499 F.3d at 634. But the Seventh Circuit also concluded that the plaintiffs in *Pisciotta* had failed to allege injury cognizable under state negligence law. This demonstrates that these are two distinct inquiries. Worix also points to *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140-41 (9th Cir. 2010), in which the court similarly found that the plaintiffs had alleged injury-in-fact for standing purposes. In an accompanying decision, however, the same court noted that its “holding that Plaintiffs-Appellants pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of their state-law claims” and found that the plaintiffs had not alleged injury under Washington negligence law. *Krottner*, 406 Fed. Appx. at 131.

Worix also relies on *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011), in which the First Circuit considered the claims of plaintiffs whose credit card data was misused by hackers who had breached a grocery store’s payment system. Although the court held that the plaintiffs had adequately alleged a negligence claim under Maine law, it specifically distinguished cases like those cited above. *Id.* at 164 (“[T]his case does not involve inadvertently misplaced or lost data which has not been

accessed or misused by third parties. Here, there was actual misuse, and it was apparently global in reach.”). Worix does not allege that his data has been misused. Thus *Anderson* does not help his case.

Worix cites no Illinois law to support his arguments. The Court finds persuasive the determination in *Rowe* that an increased risk of identity theft, even accompanied by credit-monitoring costs, does not constitute present injury under Illinois law. Worix’s attempts to distinguish his allegations from those in *Rowe* are unavailing. Moreover, he has not cited, and the Court has not found, any case from any jurisdiction holding that allegations like his are sufficient, without more, to support a state-law negligence claim. The Court therefore “decline[s] to adopt a ‘substantive innovation’ in state law or ‘to invent what would be a truly novel tort claim’ on behalf of the state absent some authority to suggest that the approval of the Supreme Court of [Illinois] is forthcoming.” See *Pisciotta*, 499 F.3d at 640 (citations omitted).

For these reasons, the Court grants MedAssets’ motion to dismiss counts two and three of Worix’s complaint. The dismissal is without prejudice: Worix may bring a claim based on these events if and when he suffers a legally cognizable injury. See *Rowe*, 2010 WL 86391 at \*6. The Court will also give Worix an opportunity to attempt to amend to allege, if he can, a present injury cognizable under Illinois law.

### **C. ICFA**

MedAssets argues that, as with Worix’s negligence claim, his failure to allege any actual damage mandates dismissal of his ICFA claim. “[P]laintiffs must allege actual damages to bring a Consumer Fraud Act action.” *Cooney v. Chi. Pub. Schs.*, 407 Ill. App. 3d 358, 365, 943 N.E.2d 23, 31 (2010) (citing 815 ILCS 505/10a(a) (“Any person

who suffers actual damage as a violation of this Act committed by any other person may bring an action against such person”).

In *Cooney*, the Illinois Appellate Court considered the claims of a group of employees whose medical information had been inadvertently disclosed to other employees. The plaintiffs argued that they had “alleged actual damages because the disclosure put them at increased risk of future identity theft” and because they had purchased credit monitoring services. *Id.* at 365-66, 943 N.E.2d at 31. Citing cases including *Williams*, *Pisciotta*, and *Rowe*, the court held that the plaintiffs’ “allegations of potential harm . . . were insufficient to support a Consumer Fraud Act claim” and that “the purchase of [credit monitoring] services, without more, is not an economic injury.” *Id.*

Another judge in this district recently considered the case of a retailer whose alleged inadequate security procedures had allowed the placement of counterfeit credit card machines in its stores, resulting in fraudulent withdrawals from customer accounts. The judge allowed the plaintiffs’ ICFA claim to proceed based on their allegations regarding fraudulent withdrawals. He noted, however, that under *Cooney*, their alleged “increased risk of identity theft, including the present and future costs of credit monitoring services” could not constitute actual damage under the ICFA. *In re Michaels Stores Pin Pad Litig.*, \_\_\_ F. Supp. 2d \_\_\_, No. 11 C 3350, 2011 WL 5878373, at \*6 (N.D. Ill. Nov. 23, 2011).

Although Worix alleges in his ICFA claim (unlike in his negligence claims) that he suffered “actual damages including lost money and property,” Compl. ¶ 62, the allegation is conclusory, and there is no indication anywhere in the complaint of what

“money or property” he might have lost as a result of MedAssets’ alleged actions. This vague and conclusory phrase does not distinguish Worix’s allegations of damages for purposes of the ICFA from the non-cognizable injury he claims to have suffered due to MedAssets’ negligence.

“[W]hen the intermediate appellate courts of the state have spoken to [an] issue, [a federal court] shall give great weight to their determination about the content of state law, absent some indication that the highest court of the state is likely to deviate from those rulings.” *Pisciotta*, 499 F.3d at 635. The Court finds the analysis of *Cooney* in *In re Michaels* to be persuasive and concludes that Worix’s allegations are insufficient to establish injury under the ICFA.

For these reasons, the Court grants MedAssets’ motion to dismiss count four of Worix’s complaint. As with its dismissal of Worix’s negligence claims, this dismissal is without prejudice.

The Court acknowledges that MedAssets did not raise the issue of actual damages under the ICFA until its reply brief and that Worix therefore did not have the opportunity to respond to its arguments on this point. Because *Cooney* constitutes clear Illinois precedent on the issue, and because courts’ analyses of actual damages under the ICFA appear to track the injury analysis on related negligence claims in similar circumstances, the Court does not expect that additional argument would have altered its determination on this point. The Court will nonetheless entertain a motion to reconsider that contains any substantive argument Worix wishes to make regarding whether he has alleged actual damages under the ICFA.

### **Conclusion**

For the reasons stated above, the Court grants MedAssets' motion to dismiss plaintiff's complaint [docket no. 10]. The dismissal of counts two, three, and four is without prejudice. Unless Worix files, by March 22, 2012, a motion for leave to amend that includes a proposed complaint that states a viable claim, the Court will enter judgment consistent with the present decision.

\_\_\_\_\_  
s/ Matthew F. Kennelly  
MATTHEW F. KENNELLY  
United States District Judge

Date: March 8, 2012