

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

BARBARA MACHOWICZ, individually	)	
and on behalf of all others similarly situated,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	No. 14 C 1394
KASPERSKY LAB, INC.	)	
	)	
Defendant.	)	
	)	

MEMORANDUM OPINION AND ORDER

JAMES F. HOLDERMAN, District Judge:

On January 27, 2014, plaintiff Barbara Machowicz (“Machowicz”) filed this putative class action against computer security software developer Kaspersky Lab, Inc. (“Kaspersky”) in the Circuit Court of Cook County, Illinois. Defendant Kaspersky removed the case to this court pursuant to 28 U.S.C. § 1332 and 28 U.S.C. § 1446(a). This court has subject matter jurisdiction under the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d)(2)(A). Machowicz sought no remand.

Machowicz’s three-count class action complaint (“Complaint”) (Dkt. No. 1 Ex. 1 (“Compl.”)) alleges Kaspersky fraudulently induced her to buy its security software through a free program called Kaspersky Security Scan (“KSS”), which is purportedly designed to “detect unwanted malware, software vulnerabilities, and other non-malware security problems.” (Compl. ¶ 1.) Machowicz alleges that KSS is essentially “scareware” engineered to detect fake security threats and trick average consumers into buying one of Kaspersky’s paid security products. (*Id.* ¶¶ 2-3.) Machowicz’s Complaint claims a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (“ICFA”), 815 ILCS 505/1, *et seq.* (Count I), fraudulent

inducement (Count II), and unjust enrichment (Count III). (*Id.* ¶¶ 53-77.)

Kaspersky has moved to dismiss all of Machowicz’s claims on the grounds that Machowicz’s Complaint fails to state a claim upon which relief can be granted. (Dkt. No. 18.) Kaspersky has also moved to strike Machowicz’s class action allegations or, in the alternative, to limit the scope of the putative class. (Dkt. No. 21.) For the reasons explained below, both motions are denied.

#### FACTUAL BACKGROUND ALLEGED IN MACHOWICZ’S COMPLAINT

Founded in 1997, Kaspersky develops and sells enterprise and consumer computer security software. (Compl. ¶ 8.) Kaspersky’s consumer security software, which generally costs between \$40 and \$60 dollars, includes Kaspersky Internet Security, Kaspersky Total Security, and Kaspersky Anti-Virus. (*Id.* ¶ 9.) To demonstrate the supposed necessity of its software, Kaspersky offers KSS as a free download to prospective customers. (*Id.* ¶ 10.) KSS, according to Kaspersky’s website, “checks for known malware and security vulnerabilities—plus advises you on your PC’s security status.” (*Id.* ¶ 11.) KSS also purports to “provide[ ] advice on how to remedy security problems that have been identified by [KSS].” (*Id.* ¶ 12.) That advice, naturally, includes the purchase of one Kaspersky’s paid security products. (*Id.*)

Machowicz alleges that Kaspersky’s seemingly legitimate marketing scheme is actually a “scareware” scam. According to Machowicz’s Complaint, Kaspersky purposefully engineered KSS to “invariably and falsely report security threats,” thereby inducing customers, like Machowicz, to pay for one of Kaspersky’s computer security products. (Compl. ¶ 12.)

In September 2013, Machowicz searched the Internet for software to optimize and protect her computer and viewed an advertisement for Kaspersky’s free KSS program. (*Id.* ¶ 38.) After reading representations in Kaspersky’s advertisement and on its website that KSS would detect

malware, other security threats, and report on her PC's security status, Machowicz downloaded KSS and conducted a "scan" of her computer. (*Id.* ¶¶ 39-41.) Upon completion of the scan, KSS reported "PROBLEMS FOUND!" and informed Machowicz that her "computer could be at risk." (*Id.* ¶¶ 33 Fig. 2, 41.) KSS also provided a button labeled "CLICK FOR A SOLUTION," which directed Machowicz to Kaspersky's website. (*Id.* ¶¶ 33 Fig. 2, 42.) The website displayed Kaspersky's security product suite and contained the following representations: (1) "[KSS] found a potential vulnerability that could put your PC at risk," (2) "Kaspersky products provide recommendations on how to fix these issues," and (3) "PURCHASE A SECURITY SOLUTION NOW." (*Id.* ¶¶ 16 Fig. 5, 42.)

Based on these representations and her belief that KSS detected genuine security issues on her computer, Machowicz purchased Kaspersky's Internet Security software for \$54.95. (*Id.* ¶ 43.) Machowicz was ultimately unhappy with her purchase and suspected that KSS reported false "problems" to trick her into paying for one of Kaspersky's full-fledged security products. (*Id.* ¶ 44.) She contacted Kaspersky to complain about KSS's misrepresentations and request a refund, but Kaspersky refused. (*Id.* ¶ 45.)

Machowicz, through her counsel, later investigated the functionality of KSS using a brand new computer. (Dkt. No. 29 ("Pl.'s Resp.") at 5.) She downloaded KSS onto the new computer and ran a scan. (Compl. ¶ 15.) Machowicz discovered that, even on a brand new computer, KSS always reports "PROBLEMS FOUND!" and informs the user that "[y]our computer could be at risk." (*Id.* ¶ 15.) Machowicz alleges that these purported "problems," which KSS characterizes as "vulnerabilities associated with the settings of installed applications and the operating system," do not pose any credible threat to a computer's security. (*Id.* ¶¶ 18-19.)

First, KSS reports vulnerabilities if a computer's "AutoRun" configuration setting is not

switched to “Off.” (*Id.* ¶ 21.) Machowicz concedes that the AutoRun setting poses security risks to computers running “older” versions of Microsoft Windows, but alleges that “newer” versions of Windows contain safeguards to eliminate those threats. (*Id.* ¶¶ 21-22.) KSS, however, reports the AutoRun “issues” as vulnerabilities without ever checking the version of Windows installed on the PC.<sup>1</sup> (*Id.* ¶ 23.)

Second, KSS reports several vulnerabilities associated with the default settings of Microsoft’s Internet Explorer and Windows Explorer. (*Id.* ¶ 24.) Machowicz alleges these default settings pose no credible threat to a computer’s security and Kaspersky apparently agrees—its website classifies six of the purported “vulnerabilities” as “Not very dangerous. Not necessary to be fixed.” (*Id.* ¶ 25.) In other words, KSS encourages customers to purchase a “security solution” for purported vulnerabilities that Kaspersky itself states are “not necessary to be fixed.” (*Id.*)

Third, Machowicz alleges that KSS reports multiple vulnerabilities associated with a single Windows setting relating to the display of file type extensions. (*Id.* ¶ 26.) Machowicz contends that the only purpose of KSS’s alleged “double-counting” is to artificially inflate the number of vulnerabilities and frighten users into buying a security solution. (*Id.* ¶ 26.)

Fourth, KSS reports that cookies placed on a user’s computer by Kaspersky’s own website are threatening vulnerabilities. (*Id.* ¶¶ 27-31.) When a user reaches Kaspersky’s website, which he or she must visit to download KSS, Kaspersky places several cookies on the user’s computer. (*Id.* ¶ 28.) KSS subsequently detects these cookies (along cookies from other websites) and reports them as vulnerabilities affecting the security of the computer. (*Id.* ¶ 29.)

---

<sup>1</sup> Machowicz has failed to identify (i) the version of Windows installed on her computer in September 2013, (ii) the version of Windows installed on her “brand new” test computer, and (iii) the specific versions of Windows susceptible or immune to AutoRun threats, although this last fact likely requires discovery.

And, like the other vulnerabilities that require fixing, KSS advises the user to purchase Kaspersky's software to eliminate the threat its own cookies purportedly pose. (*Id.*) Consequently, according to Machowicz's Complaint, KSS will *always* display a "PROBLEMS FOUND!" message because the mere act of downloading KSS creates a "vulnerability." (*Id.* ¶ 30.)

As stated earlier, Machowicz filed her class action Complaint against Kaspersky in the Circuit Court of Cook County, Illinois on January 27, 2014, alleging claims for a violation of the ICFA, fraudulent inducement, and unjust enrichment. (Compl. ¶¶ 53-77.) On February 26, 2014, Kaspersky removed the case to this federal court pursuant to 28 U.S.C. § 1332 and 28 U.S.C. § 1441(a) and (b). (Dkt. No. 1.) On April 18, 2014, Kaspersky filed its motion to dismiss Machowicz's Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6), (Dkt. No. 18), and its motion to dismiss or strike the class action allegations or, in the alternative, to limit the scope of the putative class, (Dkt. No. 21), which the parties have briefed.

#### LEGAL STANDARDS

Under the Federal Rules of Civil Procedure, a complaint need contain only "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). The complaint must "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). Although "detailed factual allegations" are not required, "labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555. The complaint must "include sufficient facts 'to state a claim for relief that is plausible on its face.'" *Cole v. Milwaukee Area Tech. Coll. Dist.*, 634 F.3d 901, 903 (7th Cir. 2011) (quoting *Justice v. Town of Cicero*, 577 F.3d 768, 771 (7th Cir. 2009)). "A claim

has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In ruling on a Rule 12(b)(6) motion, the court “construe[s] the . . . [c]omplaint in the light most favorable to Plaintiff, accepting as true all well-pleaded facts and drawing all possible inferences in his favor.” *Cole*, 634 F.3d at 903.

## ANALYSIS

### I. Rule 9(b) Heightened Pleading Standard

Machowicz’s three claims arise out of the same basic allegation: that Kaspersky offered consumers free software—KSS—that was intentionally designed to report fake or exaggerated security threats on users’ computers in order to deceive consumers into unnecessarily purchasing Kaspersky’s security software. Kaspersky argues that all of Machowicz’s claims sound in fraud and must be dismissed because Machowicz has not pled her claims with the particularity required under Federal Rule of Civil Procedure 9(b). (Dkt. No. 19 (“Def.’s Mem.”) at 9.) Under Rule 9(b), a plaintiff must plead the “circumstances constituting fraud” with particularity. These circumstances include “the identity of the person who made the misrepresentation, the time, place, and content of the misrepresentation, and the method by which the misrepresentation was communicated to the plaintiff.” *Vicom, Inc. v. Harbridge Merch. Servs., Inc.*, 20 F.3d 771, 777 (7th Cir. 1994). In other words, a plaintiff must allege “the who, what, when, where, and how.” *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 569 (7th Cir. 2012) (citations and quotations omitted).

Kaspersky maintains that Machowicz’s Complaint does not meet Rule 9(b)’s heightened pleading requirement for the following reasons: (1) failure to identify what vulnerabilities KSS falsely reported as existing on Machowicz’s computer; (2) failure to explain why or how the

vulnerabilities KSS reported on Machowicz's computer were false; and (3) failure to explain that the vulnerabilities KSS reported on Machowicz's computer were not, in fact, vulnerabilities. As Kaspersky itself concedes, all of these purported deficiencies are essentially the same argument: that Machowicz's Complaint fails to identify a false statement contained in KSS's vulnerability report for *her* computer in September 2013. (Def.'s Mem. at 11.) Kaspersky likewise contends that Machowicz cannot rely on her examination of KSS's functionality using a different, brand new a computer to satisfy the Rule 9(b) requirements for her individual claim.

Kaspersky's argument misconstrues the fraud inquiry at this stage of the litigation. Machowicz's Complaint alleges that her post-purchase investigation, not the status of her computer in September 2013, revealed the falsity of Kaspersky's and KSS's reported vulnerabilities. (Compl. ¶¶ 15-34.) Specifically, her investigation revealed that Kaspersky intentionally engineered KSS to always report "PROBLEMS FOUND!" regardless of whether any problems actually exist. (Compl. ¶ 2, 15.) Machowicz believes that KSS reported false vulnerabilities on *her* computer because, according to her investigation, KSS is rigged to always report false vulnerabilities. Whether the reported vulnerabilities actually existed on Machowicz's computer in September 2013 is a question of fact properly reserved for discovery. At the motion to dismiss stage, Machowicz's forensic investigation is sufficient to establish a basis for believing that her September 2013 report—like every other KSS report—contained fake or exaggerated vulnerabilities.

As a practical matter, without additional investigation, few plaintiffs would likely identify the precise problems initially reported by KSS on their own computers. The KSS report, along with its allegedly fake security threats, disappears once the user buys Kaspersky's paid software. For this reason, district courts faced with similar scareware allegations have uniformly

allowed plaintiffs to rely on forensic examinations of the software's functionality to satisfy the requirements of Rule 9(b). *See Beaton v. SpeedyPC*, No. 13 C 8389, 2014 WL 4376219, \*3 (N.D. Ill. Sept. 2, 2014) (Wood, J.) (rejecting argument that there was no link between forensic examination and plaintiff's personal experience); *Hall v. Tune Up Corp.*, No. 13 C 1804, 2013 WL 4012642, \*3 (N.D. Ill. Aug. 6, 2013) (Der-Yeghiayan, J.) (finding forensic examination of software sufficient to support allegations of fraud under Rule 9(b)); *Worley v. Avanquest N.A., Inc.*, No. 12 C 4391, 2013 WL 1820002, \*3 (N.D. Cal. Apr. 30, 2013) ("actual state of plaintiffs' own computers prior to and after defendant's software was used" is a matter for discovery); *Gross v. Symantec Corp.*, No. 12 C 154, 2012 WL 3116158, \*3 (N.D. Cal. July 31, 2012) ("As Plaintiff's belief derives from the results of the forensic analysis, the allegations in the [complaint] sufficiently establish a basis for believing Symantec's statements to be false.") Accordingly, Machowicz's failure to plead facts relating to the actual security status of her own PC in September 2013 is not fatal to her case at the motion to dismiss stage.

## II. ICFA and Fraudulent Inducement (Counts I and II)

Kaspersky contends, almost entirely for the reasons discussed above, that Machowicz fails to state a claim under the ICFA and for fraudulent inducement. To state an ICFA claim, a plaintiff must allege: "(1) a deceptive act or practice by the defendant, (2) the defendant's intent that the plaintiff rely on the deception, (3) the occurrence of the deception in the course of conduct involving trade or commerce, and (4) actual damage to the plaintiff (5) proximately caused by the deception." *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 574 (7th Cir. 2012) (citations omitted). Similarly, under Illinois common law, a claim for fraudulent inducement requires "(1) a false statement of material fact; (2) known or believed to be false by the person making it; (3) an intent to induce the other party to act; (4) action by the other party in reliance



on the trust of the statement; and (5) damage to the other party resulting from such reliance.” *Hoseman v. Weinschneider*, 322 F.3d 468, 476 (7th Cir. 2003) (citations omitted).

Here, Machowicz alleges that Kaspersky advertised that KSS would “check for known malware and security vulnerabilities,” but instead reported false, exaggerated or—in the case of the dangerous Kaspersky cookies—planted vulnerabilities to induce Machowicz to purchase one of Kaspersky’s paid security products. Machowicz further alleges that, in deciding to pay \$54.95 for Kaspersky Internet Security, she relied on (i) KSS’s (false) representation that her computer contained “PROBLEMS!” and “could be at risk,” (ii) that the reported problems were legitimate security threats and (iii) Kaspersky’s representation that its paid security products would “fix these issues.” In light of these factual allegations, the court finds that Machowicz’s Complaint adequately pleads a claim under the ICFA and for fraudulent inducement.<sup>2</sup>

### III. Unjust Enrichment (Count III)

Kaspersky argues that Machowicz’s unjust enrichment claim should be dismissed because her Complaint insufficiently pleads the factual allegations supporting her claims for fraud. Unjust enrichment is generally an independent cause of action under Illinois law. *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 516 (7th Cir. 2011) (citing *Raintree Homes, Inc. v. Vill. of Long Grove*, 807 N.E.2d 439, 445 (Ill. 2004)). If the unjust enrichment claim is premised on the same allegedly improper conduct as another claim, however, the unjust enrichment claim will “stand or fall” with the related claim. *Id.* at 517. Here, the parties concede that Machowicz’s unjust enrichment claim is premised on Kaspersky’s allegedly fraudulent conduct relating to

---

<sup>2</sup> Kaspersky also argues that Machowicz fails to state a claim under the unfairness prong of the ICFA, which is not subject to the heightened pleading standards of Rule 9(b). Because the court finds that Machowicz adequately alleges a claim under the deception prong of the ICFA, and thus states a claim for a violation of the ICFA, the court need not address whether Kaspersky’s alleged conduct satisfies the unfairness prong of the statute.

KSS and the representations on Kaspersky's website. Accordingly, because the court finds that Machowicz has adequately alleged a claim for fraud, her unjust enrichment claim must survive as well.

#### IV. Motion to Strike Class Allegations

The only remaining issue is Kaspersky's motion to strike Machowicz's class allegations or, in the alternative, limit the scope of the putative class. (Dkt. No. 21.) Machowicz filed her Complaint on behalf of herself and a class of similarly situated individuals, defined as: "All individuals and entities that purchased any of Kaspersky's software after using KSS." (Compl. ¶ 47.)

Federal Rule of Civil Procedure 23(c)(1)(A) provides that "[a]t an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action." Although "[m]ost often it will not be 'practicable' for the court to do that at the pleading stage . . . sometimes the complaint will make it clear that class certification is inappropriate." *Hill v. Wells Fargo Bank, N.A.*, 946 F. Supp. 2d 817, 829-33 (N.D. Ill. 2013) (Feinerman, J.) (citing *General Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 160 (1982)); *see also Kasalo v. Harris & Harris*, 656 F.3d 557, 563 (7th Cir. 2011) ("Consistent with [Rule 23(c)(1)(A)'s] language, a court may deny class certification even before the plaintiff files a motion requesting certification."). Accordingly, in limited situations, a court may determine that class certification is inappropriate even before the parties proceed to discovery. *See Bohn v. Boiron, Inc.*, No. 11 C 8704, 2013 WL 3975126, \*5 (N.D. Ill. Aug. 1, 2013) (Durkin, J.).

In this district, judges have generally addressed class certification at the pleading stage only when the class allegations are "facially and inherently deficient." *Buonomo v. Optimum Outcomes, Inc.*, No. 13 C 5274, 2014 WL 1013841, \*2 (N.D. Ill. Mar. 17, 2014) (St. Eve, J.); *see*

also *Wolfkiel v. Intersections Ins. Servs. Inc.*, No. 13 C 7133, 2014 WL 866979, \*4 (N.D. Ill. Mar. 5, 2014) (Zagel, J.); *Wright v. Family Dollar, Inc.*, No. 10 C 4410, 2010 WL 4962838, \*1 (N.D. Ill. Nov. 30, 2010) (Gettleman, J.); *Muehlbauer v. General Motors Corp.*, 431 F. Supp. 2d 847, 870 (N.D. Ill. 2006) (Moran, J.). If “discovery is needed to determine whether a class should be certified,” however, a motion to strike the class allegations at the pleading stage is premature. *See Buonomo*, 2014 WL 1013841, at \*2 (citations omitted); *see also Boatwright v. Walgreen Co.*, No. 10 C 3902, 2011 WL 843898, \*2 (N.D. Ill. Mar. 4, 2011) (Castillo, J.) (“Because a class determination decision generally involves considerations that are enmeshed in the factual and legal issues comprising the plaintiff’s cause of action . . . a decision denying class status by striking class allegations at the pleading stage is inappropriate.”)

Kaspersky contends that class certification is inappropriate because common issues of fact do not predominate over questions affecting individual members, which is a requirement for class certification under Rules 23(b)(2) and (3). (Def.’s Mem. at 4.) Kaspersky argues that the accuracy of KSS’s reported vulnerabilities depends on the user’s operating system and specific setup, which is unique to each class member’s computer. Specifically, although one of KSS’s purportedly false vulnerabilities—the AutoRun setting—is not a security threat to users with “newer” versions of Windows, the same issue represents a legitimate security concern for users of “older” versions of Windows. Kaspersky’s argument has merit with regard to the AutoRun issue, but a number of Machowicz’s other allegations do not hinge on the setup of each class member’s computer. For example, Machowicz alleges that KSS reports cookies planted on a user’s computer by Kaspersky’s own website as threatening “vulnerabilities,” regardless of the user’s operating system. The alleged cookie scam, along with a number of other allegedly fake threats discussed in the Complaint, applies to all class members and all operating systems.

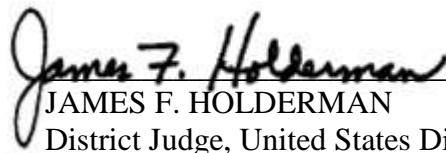
Furthermore, Machowicz alleges an overarching scheme by Kaspersky to “always” find a vulnerability on a user’s computer. KSS does not need a single, “one size fits all” vulnerability to execute its alleged scheme; it merely needs a collection of fake threats to make sure that, regardless of the user’s operating system, KSS will find *some* problem to induce the user to pay for a “solution.”

The question of which users are susceptible to which false vulnerabilities, and whether there is indeed an overarching scheme to always report “PROBLEMS FOUND!” on users’ computers, requires discovery. Accordingly, given the rigorous scrutiny that Rule 23 requires, it is too early for the court to make a determination on class certification. This court will revisit Kaspersky’s existing and additional objections to Machowicz’s class allegations if and when Kaspersky opposes Machowicz’s motion to certify the class.

#### CONCLUSION

For the reasons explained above, defendant Kaspersky’s “motion to dismiss [Machowicz’s] complaint for failure to state a claim” [18] and Kaspersky’s “motion to strike the class action allegations or in the alternative to limit the scope of the putative class” [21] are both denied. Kaspersky shall file its answer to plaintiff Machowicz’s class action complaint by 10/3/14. The court requests that counsel for the parties meet and confer pursuant to Rule 26(f). The court further requests that counsel file a joint Form 52 by 10/10/14. This case is set for a report on status and entry of a scheduling order on 10/14/14 at 9:00 a.m. The parties are encouraged to discuss settlement.

ENTER:

  
\_\_\_\_\_  
JAMES F. HOLDERMAN  
District Judge, United States District Court

Date: September 19, 2014