

Notify

✓413

16

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT.
1784CV03009-BLS2

COMMONWEALTH OF MASSACHUSETTS

v.

EQUIFAX, INC.

MEMORANDUM AND ORDER DENYING DEFENDANT'S MOTION TO DISMISS

This lawsuit concerns a massive breach of databases maintained by Equifax, Inc., as part of its credit-reporting business. Equifax collects, organizes, analyzes, and stores data concerning individual consumers, and then creates and sells "credit reports" and "credit scores" for those consumers. In 2017 hackers infiltrated Equifax's computer systems. They accessed and presumably stole credit card numbers and other personal identifying information belonging to millions of people.

The Commonwealth of Massachusetts, acting through its Attorney General, has sued Equifax on behalf of Massachusetts residents whose personal information was stolen. The Commonwealth alleges that Equifax failed to properly safeguard its databases and failed to provide prompt notice of the data breach. It asserts claims under G.L. c. 93H (the Massachusetts Data Breach Notification Law), 201 C.M.R. § 17.00 et seq. (the Massachusetts Data Security Regulations), and G.L. c. 93A (the Massachusetts Consumer Protect Act).

Equifax seeks to dismiss all claims against it under Mass. R. Civ. P. 12(b)(6). The Court will DENY this motion because the Commonwealth alleges facts plausibly suggesting that Equifax violated Massachusetts law by not taking reasonable steps to protect personal information and by not promptly informing Massachusetts consumers about and taking adequate steps to remedy the data breach.¹

¹ See generally *Lopez v. Commonwealth*, 463 Mass. 696, 701 (2012) (to survive a motion to dismiss under Mass. R. Civ. P. 12(b)(6), a complaint or counterclaim must allege facts that, if true, would "plausibly suggest[] ... an entitlement to relief") (quoting *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 636 (2008), and *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)).

Notice
Smt
4-3-18
OAG
SEC
ML
OACM#
JR
HIS
JAL
JTN
KPO
(UB)

1. Claims under G.L. c. 93H and the Implementing Regulations.

1.1. Count II Adequately Alleges Violation of Data Security Regulations.

Count II of the Commonwealth's complaint alleges that Equifax failed to develop, implement, and maintain an adequate written information security program (or "WISP"), and that this failure made the data breach possible. In particular, the complaint alleges that Equifax knew or should have known by March 7, 2017, that there was a serious security vulnerability in certain open-source computer code that Equifax used in its systems, that Equifax could have but failed to patch or upgrade its software to eliminate this vulnerability, and that as a direct result hackers accessed and stole personal information from Equifax's databases. The complaint also alleges that Equifax did not even take reasonable steps to determine whether unauthorized parties were infiltrating its computer systems. The Commonwealth alleges that these failures by Equifax violated 201 C.M.R. §§ 17.03 and 17.04.

These allegations state a viable claim for violation of the data security regulations. The Court agrees with Equifax that the mere existence of a data breach "does not translate into a violation of Chapter 93H or the Data Security Regulations." But here the Commonwealth alleges that Equifax knew for months it needed to patch its open-source code in order to keep its databases secure—or at least that it should have been aware that the software provider had provided public notice of the software vulnerability and how to fix it—and that it failed to do so. These allegations plausibly suggest that Equifax breached its legal duties to address all reasonably foreseeable risks to its data security under 201 C.M.R. § 17.03(2)(b), and to implement reasonably up-to-date patches to its software under 201 C.M.R. § 17.04(6) and (7).

Equifax argued for the first time during oral argument that these regulations cannot be applied here because: (i) the statute distinguishes between and imposes different data breach disclosure obligations upon someone "that owns or licenses data that includes personal information," on the one hand, and someone "that maintains or stores, but does not own or license" such data, see G.L. c. 94H, § 3; (ii) the Legislature authorized the Department of Consumer Affairs and business Regulation (the "Department") to "adopt regulations relative to any person that owns or licenses personal information of residents of the commonwealth," but did not authorize data

other personal information. All of these subsidiary allegations readily support the Commonwealth's express allegation that "Equifax owned or licensed personal information of at least one Massachusetts resident."

An entity that creates and owns proprietary databases containing consumers' personal information would appear to "own" that information within the meaning of G.L. c. 93H. As noted above, the statute distinguishes entities that merely "maintain" or "store" personal information from those that have an ownership interest in the data. Companies that offer cloud storage services, for example, may and probably do maintain and store personal information that they cannot sell or otherwise control as owners. In contrast, Equifax allegedly maintains its own proprietary database and sells reports containing consumers' personal information.

These allegations plausibly suggests that Equifax should be treated as an "owner" of this database and the personal information it contains for the purposes of G.L. c. 93H, even if the underlying data themselves belong to someone else or have been shared and thus are no longer confidential.³ Compare *New England Overall Co. v. Woltmann*, 343 Mass. 69, 77 (1961) (employer had proprietary interest in confidential customer database) with *American Window Cleaning Co. of Springfield, Mass. v. Cohen*, 343 Mass. 195, 199 (1961) ("Remembered information as to the plaintiff's prices, the frequency of service, and the specific needs and business habits of particular customers was not confidential") and *DiAngeles v. Scauzillo*, 287 Mass. 291, 297-298 (1934) (employer may own written list of customers, even though it cannot own employee's memory or personal notes of client information).

1.2. Count I Adequately Alleges Untimely Disclosure. Count I alleges that Equifax violated the Massachusetts Data Breach Statute by failing to provide prompt notice to the Attorney General, the Department, and affected individual consumers about the data breach. The Commonwealth alleges that Equifax knew or should have known about the data breach by July 29, 2017, and that Equifax waited to provide the required notice until September 7, 2017. It further alleges that Equifax

³ The Court therefore need not and does not reach the Commonwealth's further argument that the Department's authority to promulgate data security regulations is not limited to entities that own or license personal information, but extends to entities that only maintain or store such data.

did not provide notice “as soon as practicable and without unreasonable delay,” as required by G.L. c. 93H, § 3(b).⁴

Equifax argues that the facts alleged in the complaint do not plausibly suggest that it failed to give the required notice of the data breach without unreasonable delay.

This is not an issue that can be resolved on a motion to dismiss. “[T]he question what constitutes a reasonable time is normally treated as one for the finder of fact;” it is not a question of law that can be decided on a motion to dismiss. See *Cablevision of Boston, Inc. v. Shamatta*, 63 Mass. App. Ct. 523, 526, rev. denied, 444 Mass. 1105 (2005); accord *Loranger Const. Corp. v. E. F. Hauserman Co.*, 6 Mass. App. Ct. 152, 158 (1978). The same is true where a party has a duty to provide notice within a reasonable time after they knew or should have known that some event or condition has occurred. In such a case, “[w]hether the notice was given within a reasonable time was a question of fact” to be decided at trial. *Johnson v. Kanavos*, 296 Mass. 373, 377 (1937); accord *Fortin v. Ox-Bow Marina, Inc.*, 408 Mass. 310, 315 (1990).

1.3. Non-Compliance with Federal Law Is Not an Element. In addition, Equifax seeks dismissal of Counts I and II on the alternative ground that the Commonwealth failed to allege that Equifax was not in compliance with federal law.

The data breach act provides that “a person who maintains procedures for responding to breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs...” G.L. c. 93H, § 5.

The Commonwealth is not required to allege or prove non-compliance with federal rules as an element of a claim under the data breach statute, however.

Instead, any assertion by Equifax that it is exempt from liability under the statute or regulations, because of the separate safe harbor provision of § 5, is an affirmative defense that must be pleaded and proved by Equifax. “Generally, the party claiming an exemption from the provisions of a statute has the burden to show

⁴ The Legislature has authorized the Attorney General to bring suit under G.L. c. 93A, § 4, “to remedy violations of” the Data Breach Statute. See G.L. c. 93H, § 6.

that it is entitled to the exemption.” *Goodrow v. Lane Bryant, Inc.*, 432 Mass. 165, 170 (2000) (employer had burden of proving claimed exemption from overtime pay statute). Thus, where a statute imposes some “duty or obligation,” and a “separate or distinct clause or statute” creates an exception to the general rule of liability, “then the party relying on such exception must allege and prove it.” *Ansell v. City of Boston*, 254 Mass. 208, 211 (1926); accord *Afienko v. Harvard Club of Boston*, 365 Mass. 320, 331 (1974).

2. Claims under G.L. c. 93A.

2.1. Count III Adequately Alleges Violations of c. 93H. In Count III, the Commonwealth alleges that every violation of 201 C.M.R. §§ 17.03-17.04 and of G.L. c. 93H is a separate violation of G.L. c. 93A, and that as a result Equifax should be ordered to pay civil penalties, attorneys’ fees and costs; to disgorge profits obtained as a result of the data breach; and to comply with a permanent injunction.

Equifax argues that Count III is completely derivative of the claims asserted in Counts I and II, and thus that if the claims under the data security regulations and the data breach act are dismissed the related claim under Count III must also be dismissed. Cf. *Park Drive Towing, Inc. v. City of Revere*, 442 Mass. 80, 85-86 (2004) (where c. 93A claim is based on and derivative of some underlying claim that fails as a matter of law, that 93A claim “must also fail”).

But the Court concludes, as explained above, that Counts I and II state viable claims. It follows that Equifax has not shown any ground for dismissing Count III.

2.2. Count IV Adequately Alleges Deceptive Misrepresentations. Count IV alleges that Equifax engaged in unfair or deceptive conduct in violation of G.L. c. 93A by making misrepresentations regarding its efforts to protect personal information held in its databases. According to the Commonwealth, Equifax represented to consumers that it would maintain “reasonable, physical, technical and procedural safeguards to help protect your personal information.” But, the Commonwealth alleges, these representations were false and deceptive, because Equifax actually knew it was not taking all reasonable steps to patch its software and protect the personal information contained in its databases.

Equifax argues that this claim should be dismissed for three different reasons. None has merit.

First, Equifax argues that the Commonwealth may not sue for a violation of c. 93A based only on allegations that the efforts made by Equifax to keep its databases secure proved to be inadequate.

The legal premise of this argument is correct as far as it goes. “[A] violation of G.L. c. 93A requires, at the very least, more than a finding of mere negligence.” *Boyle v. Zurich American Ins. Co.*, 472 Mass. 649, 662 (2015), quoting *Darviris v. Petros*, 442 Mass. 274, 278 (2004). Thus, “a negligent miscalculation” that involved no kind of willful or knowing misrepresentation or deceit does not violate c. 93A. *Id.*

But the Commonwealth alleges more than mere negligence. As explained above, it alleges that Equifax deceived consumers by asserting that it was taking all reasonable steps to keep its data secure when Equifax knew that was not true.

Those allegations plausibly suggest that Equifax engaged in the kind of unfair or deceptive misrepresentations that violate c. 93A. “A negligent misrepresentation of fact may ... constitute an unfair or deceptive act within the meaning of G.L. c. 93A, if the truth could have been reasonably ascertained.” *Quinlan v. Clasby*, 71 Mass. App. Ct. 97, 102, rev. denied, 451 Mass. 1103 (2008); accord, e.g., *Briggs v. Carol Cars, Inc.*, 407 Mass. 391, 396-397 (1990); *Golber v. BayBank Valley Trust Co.*, 46 Mass. App. Ct. 256, 261 (1999); *Glickman v. Brown*, 21 Mass. App. Ct. 229, 235 (1985). It would therefore be reversible error to dismiss a c. 93A claim based on plausible allegations, like those in this case, that a participant in trade or commerce used negligent misrepresentation to deceive consumers. *Marram v. Kobrick Offshore Fund, Ltd.*, 442 Mass. 43, 62 (2004) (reversing dismissal).

Second, Equifax argues that at least some of its public representations regarding keeping consumers’ information secure were mere “puffery” that no reasonable person would take seriously.

This is yet another issue that cannot be resolved as a matter of law and therefore cannot be resolved on a motion to dismiss. See *Marram, supra* (reversing Rule 12(b)(6) dismissal of claim under G.L. c. 93A because whether statements by defendant “are unactionable ‘mere puffery’ ” could not be resolved on the pleadings).

Third, Equifax argues that the Commonwealth has not alleged facts plausibly suggesting that the alleged misrepresentations caused Massachusetts consumers to suffer any actual economic injury.

This argument fails because the Attorney General, unlike a private litigant who sues under § 9 or § 11 of c. 93A, is only required to prove that unfair or deceptive acts or practice took place in trade or commerce; she is not required to prove or quantify resulting economic injury. The Attorney General may seek injunctive relief or civil penalties “[w]hensoever” she “has reason to believe that any person is using or is about to use” an unfair or deceptive act or practice in violation of the consumer protection act. See G.L. c. 93A, § 4. She is not required to allege or prove that any individual consumer was actually harmed by the allegedly unfair or deceptive act or practice. See *Commonwealth v. Fall River Motor Sales, Inc.*, 409 Mass. 302, 312 (1991); *Commonwealth v. Chatham Development Co., Inc.*, 49 Mass. App. Ct. 525, 528-529, rev. denied, 432 Mass. 1107 (2000).

2.3. Count V's Allegations of Inadequate Response Are Not Moot.

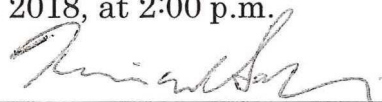
Finally, Count V alleges that Equifax has not taken adequate steps to mitigate all the harm caused by the data breach, and that its failure to do so is an unfair or deceptive act or practice that violates G.L. c. 93A.

Equifax disagrees. It insists that its remedial efforts have been more than adequate, and that Count V is therefore moot.

Whether a violation of the consumer protection act has been adequately and completely remedied is not something that can be resolved on a motion to dismiss. Indeed, Equifax fails to cite a single appellate decision affirming or requiring dismissal of a c. 93A on this ground.

ORDER

Defendant's motion to dismiss is DENIED. The Court will hold a Rule 16 scheduling conference with the parties on May 1, 2018, at 2:00 p.m.



Kenneth W. Salinger
Justice of the Superior Court

2 April 2018