

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NEVILLE MCFARLANE et al., *individually and on
behalf of all others similarly situated*,

Plaintiffs,

-v-

ALTICE USA, INC.,

Defendant.

20-CV-1297 (JMF)

OPINION AND ORDER

JESSE M. FURMAN, United States District Judge:

This putative class action arises from a November 2019 data breach at Altice USA, Inc. (“Altice”), one of the largest television and communications providers in the United States. The nine named Plaintiffs are current or former employees of Altice whose personal identifying information, including Social Security numbers, was stolen in the breach. They bring various claims — for negligence, negligence *per se*, breach of implied contract, violation of the New York Labor Law, and violation of the Cable Communications Act of 1984 — against Altice for allegedly failing to take adequate measures to protect their data. Now pending are three motions filed by Altice. First, Altice moves, pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure, to dismiss for lack of subject-matter jurisdiction, on the ground that Plaintiffs fail to allege injury sufficient to give them Article III standing. Second, Altice moves, pursuant to the Federal Arbitration Act (“FAA”), 9 U.S.C. § 1 *et seq.*, to compel seven of the nine named Plaintiffs to arbitrate their claims based on a clause in the General Terms and Conditions to which they allegedly agreed as subscribers of Altice’s cable services. And third, Altice moves,

pursuant to Rule 12(b)(6), to dismiss Plaintiffs' claims under the New York Labor Law (and related claims for negligence *per se*) as well as their claims for breach of an implied contract.

Altice's motions to dismiss are relatively easily resolved. For the reasons discussed below, the Court concludes that Plaintiffs — three of whom have *already* experienced identity theft since the data breach — plainly allege the kind of injury sufficient to give them Article III standing; that their New York Labor Law claims (and related negligence *per se* claims) fail as a matter of law; and that they state plausible claims for breach of an implied contract. Altice's motion to compel arbitration requires more extensive discussion as it is based on a relatively new species of arbitration clause that one scholar has dubbed an "infinite arbitration clause" for its striking breadth: It effectively requires arbitration of *any* dispute between a subscriber and Altice, as well Altice's parents, subsidiaries, affiliates, successors, employees, agents, and the like, whether arising now or in the future, and without regard for whether it arises from or relates to the cable services agreement of which it is part. For the reasons discussed below, the Court concludes that, as a matter of either contract formation or unconscionability, the arbitration clause at issue does not require arbitration of claims that lack a nexus to the cable services agreement. Because the record is unclear with respect to whether or to what extent Plaintiffs' claims arise from or relate to their status as cable service subscribers, the Court ultimately defers decision on the motion to compel arbitration pending supplemental submissions from the parties.

BACKGROUND

The Court is technically permitted to consider materials beyond the four corners of the Amended Complaint in deciding Altice's motions to dismiss for lack of subject-matter jurisdiction and to compel arbitration. *See, e.g., Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 229 (2d Cir. 2016) (arbitration); *Cortlandt St. Recovery Corp. v. Hellas Telecomms., S.À.R.L.*, 790

F.3d 411, 417 (2d Cir. 2015) (jurisdiction). Nevertheless, the following facts are drawn from the Amended Complaint and documents that it incorporates by reference. *See DiFolco v. MSNBC Cable L.L.C.*, 622 F.3d 104, 110-11 (2d Cir. 2010).

Altice is one of the largest cable television and communications providers in the United States. *See* ECF No. 42 (“Am. Compl.”), ¶ 1. In November 2019, cyber criminals targeted Altice with a phishing attack, and an “undisclosed number” of the company’s employees inadvertently divulged the log-in credentials for their corporate email accounts. *See id.* ¶¶ 5, 99. The cyber criminals then “used the stolen credentials to remotely access and, in some instances, download the employees’ mailbox contents.” *Id.* ¶ 96; *see* ECF Nos. 42-1 (“Breach Notice”), 42-2, 42-3.¹ A forensic investigation revealed that one of the downloaded email inboxes contained a password-protected, but unencrypted, document with the names, employment information, dates of birth, social security numbers, and, in some instances, driver’s license numbers of 52,846 current and former Altice employees. *See* Am. Compl. ¶¶ 6-7, 101-02, 154, 161. In February 2020, Altice sent notices to those whose data was affected stating that, “[a]s a former [or current] employee, your personal information was included in this report.” *See id.* ¶¶ 96-97; Breach Notice. “[I]n an abundance of caution,” the notices offered recipients free identity and credit monitoring services for one year and recommended resources for monitoring and fraud protection. Breach Notice (emphasis omitted).

The named Plaintiffs in this putative class action are nine former employees of Altice or its subsidiaries or predecessor companies who received the Breach Notice. *See* Am. Compl. ¶¶ 14, 17, 22, 24, 30, 32, 38, 40, 46, 48, 54, 56, 62, 64, 70, 72, 81, 83. All but one — namely, DeAnna Cottrell — are also current or former cable subscribers through Altice or one of its

¹ ECF Nos. 42-1, 42-2, and 42-3 are substantively identical in all material respects.

subsidiaries. *See id.* ¶¶ 15, 31, 39, 47, 55, 63, 71, 82. Plaintiffs were required to provide the personal identifying data that was compromised in the breach as “a condition of their employment.” *Id.* ¶ 104. All Plaintiffs have already spent time responding to the breach, such as by regularly monitoring their accounts and credit reports, changing passwords, and implementing credit freezes. *See id.* ¶¶ 18, 26, 34, 43, 50, 59, 66, 75, 85. Because their Social Security numbers were compromised, Plaintiffs anticipate needing to monitor their identity and credit and needing to pay for identity theft protection and credit monitoring services “for the rest of [their] li[ves].” *Id.* ¶¶ 18, 26, 34-35, 43, 50-51, 59, 66-67, 76, 86.

Additionally, three of the named Plaintiffs — Neville McFarlane, Shariq Mehfooz, and Steven Paniccia — were the victims of identity theft in the months following the breach. All three allege that between December 2019 and March 2020, they discovered that identity thieves had used their personal identifying information to fraudulently open credit cards in their names. *See id.* ¶¶ 16, 73-74, 84. In March 2020, an identity thief also “attempted to change [McFarlane’s] home address.” *Id.* ¶ 16. Mehfooz discovered the fraudulent credit card application when he was applying to refinance his home mortgage. *See id.* ¶ 73. The fraudulent application harmed his credit score and interrupted the refinancing process, which may have prevented him from taking advantage of “historically low interest rates.” *Id.* ¶¶ 73-74. All three allege that, to their knowledge, they had not been the victim of any data breach other than the breach of Altice. *Id.* ¶¶ 20, 79, 88. The other six allege that they are “at imminent and substantial risk of identity theft that is continuous and ongoing.” *Id.* ¶¶ 25, 33, 42, 49, 58, 65.

The named Plaintiffs bring claims on behalf of a nationwide class of “[a]ll persons whose personally identifiable information was compromised as a result of the Data Breach at Altice USA, Inc. in November 2019.” *Id.* ¶ 170. They bring claims for negligence, *see id.* ¶¶ 181-95;

negligence *per se* for violation of the New York Labor Law, § 203-d, *see* Am. Compl. ¶¶ 196-204; negligence *per se* for violation of the Cable Communications Act of 1984, 47 U.S.C. § 551, *see* Am. Compl. ¶¶ 205-14; direct violation of the New York Labor Law, § 203-d, *see* Am. Compl. ¶¶ 215-22; direct violation of the Cable Communications Act of 1984, 47 U.S.C. § 551, *see* Am. Compl. ¶¶ 223-33; and breach of implied contract, *see id.* ¶¶ 234-39.² In addition, they seek a declaration that Altice’s existing cybersecurity measures are inadequate and an injunction requiring certain improvements. *See* Am. Compl. ¶¶ 240-46. Now pending before the Court are Altice’s motion to dismiss the Amended Complaint pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, ECF No. 45, and Altice’s motion to compel seven of the named Plaintiffs — McFarlane, Edward Hellyer, Carrie Mason-Draffen, Haseeb Raja, John Frontera, Mehfooz, and Paniccia — to submit their claims to arbitration, ECF No. 47.

SUBJECT-MATTER JURISDICTION

The Court begins, as it must, with Altice’s motion to dismiss for lack of subject-matter jurisdiction. *See, e.g., Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 94 (1998). In particular, Altice moves to dismiss on the ground that Plaintiffs lack standing, *see* ECF No. 46 (“Def.’s Mem.”), at 5-13, which is an “essential aspect” of Article III’s limitation on the “judicial Power” of the federal courts to “Cases” and “Controversies,” *Hollingsworth v. Perry*, 570 U.S. 693, 704 (2013); *see* U.S. Const. art. III, § 2. It is well established that “the irreducible constitutional minimum of standing contains three elements”: (1) injury in fact, (2) causation, and (3) redressability. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). An injury in fact is “an invasion of a legally protected interest which is (a) concrete and particularized, and (b)

² Plaintiff Cottrell, who never subscribed to cable service through Altice or any of its subsidiaries, *see* ECF No. 48 (“Def.’s Mot. to Compel Mem.”), at 1 n.1, does not join in the two claims pursuant to the Cable Communications Act of 1984, *see* Am. Compl. ¶¶ 205-13, 223-33.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.