UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NEVILLE MCFARLANE, EDWARD HELLYER, DEANNA COTTRELL, CARRIE MASON-DRAFFEN, HASEEB RAJA, RONNIE GILL, JOHN FRONTERA, SHARIQ MEHFOOZ, and STEVEN PANICCIA, individually and on behalf of all others similarly situated, Plaintiffs, v. ALTICE USA, INC., a New York Corporation, Defendant.	Lead Case No. 20-CV-1297 (consolidated with 20-CV-1410)

PLAINTIFFS' SUPPLEMENTAL MEMORANDUM
IN SUPPORT OF PRELIMINARY APPROVAL OF SETTLEMENT

Plaintiffs Neville McFarlane ("McFarlane"), Deanna Cottrell ("Cottrell"), Edward Hellyer ("Hellyer"), Carrie Mason-Draffen ("Mason-Draffen"), Haseeb Raja ("Raja"), Ronnie Gill ("Gill"), John Frontera ("Frontera"), Shariq Mehfooz ("Mehfooz"), and Steven Paniccia ("Paniccia"), individually and on behalf of the putative class, (collectively, "Plaintiffs"), submit this Supplemental Memorandum in Support of Plaintiffs' Motion for Preliminary Approval (Dkt. No. 87) ("Motion").[1]

This Supplemental Memorandum is submitted pursuant to the Court's Order of May 3, 2022 (Dkt. No. 90) in which the Court requested briefing on the issue of Plaintiffs' Article III standing. In particular, the Court referenced the Second Circuit's opinion in *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021) as well as this Court's earlier Order on standing in this action (Dkt. No. 58) and discussed the possibility that these earlier decisions may not remain good law in the aftermath of the Supreme Court's decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

While Plaintiffs understand that standing cannot be presumed, the Supreme Court's holding in *TransUnion* does ***not*** change this Court's earlier holding concerning Class Members' standing.[2] Indeed, although various courts have considered the impact of *TransUnion* on data breach cases, ***no*** court has found that *McMorris* was superseded by *TransUnion*. *See, e.g., Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *3, n.1 (S.D.N.Y. Jan. 19, 2022)

[1] Pursuant to Rule 10(c), Fed. R. Civ. P., Plaintiffs incorporate by reference Plaintiffs' Response in Opposition to Defendant's Motion to Dismiss and Motion to Compel Arbitration (Dkt. No. 54).

[2] The Court's Order references a portion of Plaintiffs' memorandum in support of preliminary approval where Plaintiffs discuss potential risks of the litigation, including the risk that Altice would continue to challenge standing. *See* Dkt. No. 90. Plaintiffs did not intend to suggest that their standing was somehow infirm under current controlling authority; however, Plaintiffs acknowledge that continuing to litigate the case (which could take years) increases the risk that new authority could emerge that Altice would use to challenge standing.

(declining to find that *TransUnion* supersedes *McMorris*); *Bohnak v. Marsh & McLennan Cos., Inc.*, No. 21-CV-6096 (AKH), 2022 WL 158537, at *4 (S.D.N.Y. Jan. 17, 2022) (finding that the exposure of plaintiffs' sensitive information to cybercriminals as a result of a targeted data breach constituted injury-in-fact even after *TransUnion*). In the absence of a clear mandate demonstrating that *McMorris* has, in fact, been overturned, the Court should continue to view *McMorris* as controlling authority. *See Bonobos*, 2022 WL 170622, at *3, n.1 ("[I]t is the task of the Second Circuit, not this Court, to determine if *McMorris* should be overturned.") (internal quotation marks omitted) (citing *United States v. Diaz*, 122 F. Supp. 3d 165, 179 (S.D.N.Y. 2015) (observing that a district court must follow a precedential opinion of the Second Circuit "unless and until it is overruled ... by the Second Circuit itself or unless a subsequent decision of the Supreme Court so undermines it that it will almost inevitably be overruled by the Second Circuit").

I. SUMMARY OF FACTUAL ALLEGATIONS

Altice USA, Inc. ("Altice" or "Defendant") is one of the largest cable TV and communications providers in the United States. Plaintiffs are current and former employees of Altice, or its affiliates, who entrusted Altice with their sensitive personally identifiable information ("PII").

In February 2020, Altice notified current and former employees (as well as the attorneys general of several states) that in November 2019, a successful phishing campaign was launched against Altice. Through this phishing scheme, cybercriminals obtained the email credentials of certain Altice employees and then used those credentials to access these employees' corporate email accounts. Once these cybercriminals were inside Altice's corporate email accounts, they were able to "access" and "download" a report containing the unencrypted PII of 52,846 current and former Altice employees, including their employment information, dates of birth, Social Security numbers,

and some drivers' license numbers (the "Data Security Incident"). *See* Second Amended Consolidated Class Action Complaint ("Complaint") (Dkt. No. 59) at ¶¶ 1-7; *id.* at Exhibits 1-3.

As a result of the Data Security Incident, Plaintiffs and the Class suffered concrete injuries, including, *inter alia*, identity theft, the exposure of their PII to cybercriminals, a substantial risk of identity theft, and actual losses. *See id.* at ¶¶ 12-87; *see also* Dkt. No. 54, at 2-13.

II. PLAINTIFFS SUFFERED INJURY-IN-FACT AND THUS HAVE ARTICLE III STANDING

To establish standing at the pleading stage, the complaint must allege facts demonstrating that the plaintiffs "have (1) suffered an injury in fact; (2) that is fairly traceable to the challenged conduct of a defendant; and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). An injury-in-fact is "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 1548.

"A party facing prospective injury has standing to sue where the threatened injury is real, immediate, and direct." *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008). An allegation of threatened injury in the future is sufficient to establish standing "if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). Supreme Court precedent does not "uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about"—hence, the "substantial risk" standard. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013). Ultimately, the purpose of the imminence requirement is "to ensure that the court avoids deciding a purely hypothetical case[.]" *Baur v. Veneman*, 352 F.3d 625, 632 (2d Cir. 2003).

Here, all Plaintiffs had their highly sensitive PII, including names, dates of birth, and Social Security numbers, exposed to and ***downloaded*** by cybercriminals due to the alleged negligence of

Altice. Complaint at ¶¶ 12-87; *see also* Exhibits 1-3 to Complaint. As a result, Plaintiffs and the Class have suffered injuries that confer Article III standing.

A. This Court's Prior Order Properly Found Standing

As part of its Order denying in part Defendant's motion to dismiss, this Court found "with little difficulty" that "all nine Plaintiffs plausibly allege injury in fact." *McFarlane v. Altice USA, Inc.*, 524 F. Supp. 3d 264, 272 (S.D.N.Y. 2021) (Dkt. No. 58, at 7). In coming to this conclusion, the Court found persuasive, *inter alia*, that "[t]hree — McFarlane, Mehfooz, and Paniccia — have already suffered concrete injury in the form of identity theft." *Id.*; *see also* Complaint at ¶¶ 16, 72, 83. The Court further found that both (i) the nature of the Data Security Incident (as a targeted phishing attack designed to extract monetizable information) and (ii) the nature of the PII exposed and downloaded (which included immutable information such as dates of birth and Social Security numbers) demonstrated that all Plaintiffs had suffered "an injury in fact within the meaning of Article III." *McFarlane*, 524 F.Supp.3d at 273 (Dkt. No. 58, at 9).

The Court's holding was well supported by numerous legal authorities. *See id.* at 271-73 (Dkt. No. 58, at 5-9) (discussing and applying relevant case law); *see, e.g., Am. Fed'n of Gov't Emps. v. Office of Pers. Mgmt* (*In re U.S. Office of Pers Mgmt. Data Sec. Breach Litig.*), 928 F.3d 42, 55-61 (D.C. Cir. 2019) (per curiam); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 387-89 (6th Cir. 2016) (unpublished); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967-68 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692-94 (7th Cir. 2015); *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 338-41 (W.D.N.Y. 2018); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017).

DOCKET ALARM

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.