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courts have considered the impact of *TransUnion* on data breach cases, ***no*** court has found that *McMorris* was superseded by *TransUnion*.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).

B. *McMorris* Supports a Finding of Standing

Shortly after this Court found that standing was sufficiently alleged in this case, the Second Circuit addressed the question of whether an increased risk of identity theft caused by a data breach creates an injury-in-fact. In *McMorris v. Carlos Lopez & Associates, LLC,* the Second Circuit held that plaintiffs alleging a risk of future harm arising out of a data breach may have standing. 995 F.3d 295, 301 (2d Cir. 2021).

The Second Circuit in *McMorris* established that courts should consider three non-exhaustive factors when analyzing whether an alleged "risk of identity theft or fraud is sufficiently 'concrete, particularized, and ... imminent.'" *Id.* (quoting *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020)). These factors are: (i) whether the data at issue has been compromised as the result of a targeted attack intended to obtain the data; (ii) whether at least some portion of the compromised dataset has been misused, even if plaintiffs' particular data has not yet used for identity theft or fraud; and (iii) whether the type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud, such as Social Security numbers and date of birth, particularly when accompanied by victims' names. *Id.* at 301-03. *McMorris* further ruled that expenses reasonably incurred to mitigate a substantial risk of future identity theft or fraud may also qualify as injury-in-fact but only where a substantial risk exists in the first instance. *Id.* at 303 (quoting *Clapper*, 568 U.S. at 416, 133 S.Ct. 1138) ("[P]laintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'").

The standard set forth in *McMorris* is satisfied here. First, a cybercriminal conducted a targeted phishing campaign on certain Altice employees, gained email credentials for those Altice employees, used those credentials to access employee emails, and then ***downloaded*** a document

containing Plaintiffs and Class Members' PII. *See* Complaint at ¶¶ 92-100; *see also* Exhibits 1-3 to Complaint. Second, three of the named plaintiffs had their PII misused within weeks or months of that same PII being accessed and downloaded by cyberhackers in the Data Security Incident. *Id.* at ¶¶ 16, 72, 83. Third, the PII that was exposed included Plaintiffs' names, Social Security numbers, and date of births. *McMorris*, 995 F.3d at 302 ("Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth – especially when accompanied by victims' names – makes it more likely that those victims will be subject to future identity theft or fraud."). Thus, Plaintiffs have demonstrated standing pursuant to the considerations set out in *McMorris*. *Id.*

Accordingly, this Court's earlier finding in *McFarlane* is reaffirmed by the Second Circuit's mandate in *McMorris*. To be sure, the factors enumerated in *McMorris* largely track the factors this Court considered and found persuasive when it concluded that Plaintiffs sufficiently alleged standing. *See McFarlane*, 524 F.Supp.3d at 271-73 (Dkt. No. 58, at 5-9). Because *McMorris* has not been clearly superseded, it continues to be controlling precedent. *Bonobos*, 2022 WL 170622, at *3, n.1.

C. *TransUnion* Does Not Compel a Different Analysis or Result

The Supreme Court's holding in *TransUnion* does not overturn the Court's prior rulings on standing in this case or in *McMorris*. Indeed, even after *TransUnion*, it remains true that "the Supreme Court has never addressed the question of whether an increased risk of identity theft caused by a data breach causes concrete or 'certainly impending' injury-in-fact[.]" *Bohnak v. Marsh & McLennan Cos., Inc.*, No. 21-CV-6096 (AKH), 2022 WL 158537, at *4 (S.D.N.Y. Jan. 17, 2022) (internal citations omitted).

The *TransUnion* opinion must be analyzed in its context. *TransUnion* involved claims for federal ***statutory violations*** for which ***statutory***—not actual—damages were sought. *See TransUnion*, 141 S.Ct. at 2205-07 (discussing standing and separation of power concerns "where a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right"). Ultimately, the Court had "no trouble concluding" that the 1,853 class members whose inaccurate credit reports were sent to third parties "suffered a concrete harm," *id.* at 2209, but found that the other 6,332 class members whose inaccurate reports were never provided to third parties "was too speculative to support Article III standing." *Id.* at 2212. The Court held that where the defendant's statutory violations resulted not in any actual harm, but ***only*** in a ***risk*** of future harm for some class members, that risk could not support those class members' standing to obtain retrospective ***statutory*** damages. *Id.* at 2210-11.

The holding and reasoning of *TransUnion* simply does not put in jeopardy the prior finding of standing in this case. Unlike the class in *TransUnion*, Plaintiffs do ***not*** seek statutory damages that are awardable for the mere technical violation of a statute absent any showing of actual injury. Instead, Plaintiffs seek to recover compensatory damages for common law claims and injunctive relief. *Cf. TransUnion*, 141 S.Ct. at 2210 (explicating that the risk of future harm alone can provide standing for injunctive relief). This is an important distinction. Indeed, under the Second Circuit's articulation of *TransUnion*, Plaintiffs' standing for their common law claims remains intact. *See Faehner v. Webcollex, LLC*, No. 21-1734-CV, 2022 WL 500454, at *1 (2d Cir. 2022) (summary order) (holding that *TransUnion* "narrowed the grounds for asserting standing ***where the injury is primarily statutory***.") (emphasis added); *see also Gilbert v. AFTRA Ret. Fund*, No. 1:20-CV-10834-ALC, 2022 WL 825489, at *3 (S.D.N.Y. Mar. 18, 2022) (allowing plaintiffs an opportunity to consider whether to replead following *TransUnion* because the "Court must be certain that each

individual named plaintiff in this action has adequately alleged Article III injury-in-fact, with the requisite concreteness, ***regarding each of their statutory claims*** for damages" but raising no such concern for plaintiffs' common law claims).

Moreover, *TransUnion* does not alter Plaintiffs' standing because the exposure of Plaintiffs' PII in the Data Security Incident created a concrete injury separate from the substantial risk of identity theft. *See TransUnion*, 141 S.Ct. at 2211 (finding that concrete harm can exist when the exposure to the risk of future harm causes a separate concrete harm). In *Bohnak*, the Southern District of New York found standing for data breach victims and held that the "exposure of Plaintiffs' PII causes a separate concrete harm, analogous to that associated with the common-law tort of public disclosure of private information." *Bohnak*, 2022 WL 158537, at *5. In arriving at this holding, the Court relied on *TransUnion*, which recognized that "[v]arious intangible harms can also be concrete…. Those include, for example, . . . disclosure of private information." *TransUnion*, 141 S.Ct. at 2204; *see Bohnak*, 2022 WL 158537, at *5. Indeed, *TransUnion* appears to support a finding of standing in this case. Here, the Class consists only of the 52,846 employees whose PII was identified by Altice and its computer forensic expert as having ***actually been exposed to***, and downloaded by, third party cybercriminals during the Data Security Incident. *See* Complaint at ¶¶ 92-100; *id.* at Exhibits 1-3. Because all Class Members had their PII accessed and downloaded by third party cybercriminals, the Class Members are analogous to the 1,853 class members in *TransUnion* who had their inaccurate reports provided to third parties and for whom the Court found a concrete injury.[3] *TransUnion*, 141 S.Ct. at 2209. In addition, the substantial

[3] Correspondingly, the 6,332 class members in *TransUnion* whose inaccurate reports were never provided to third parties would be analogous to employees who had PII stored on Altice's inadequately secured network during the Data Security Incident but whose PII was ***not*** identified as having been specifically exposed to third party cybercriminals. Plaintiffs do not allege claims on behalf of such employees.

risk of identity theft caused separate harms in the form of monetary losses. *See* Dkt. No. 54 at 10-12; *McFarlane*, 524 F. Supp. 3d at 271 (Dkt. No 58, at 6) ("[A] substantial risk of harm 'may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm,' which costs can themselves constitute an injury in fact.") (quoting *Clapper*, 568 U.S. at 414 n.5, 133 S.Ct. 1138).

In sum, *TransUnion's* holding that a mere risk of future harm that never materializes is insufficient concrete harm to provide standing for retrospective statutory damages does not overturn the holdings of *McFarlane* or *McMorris*. First, Plaintiffs' claims are not premised on a damages remedy divorced from actual harm suffered, as is the case where statutory damages are awardable merely upon the violation of a statute. Second, because Defendant cannot change the fact that an unauthorized cybercriminal conducted a phishing scheme on Altice employees, gained email credentials for certain Altice employees, used those credentials to access employee emails, and then ***downloaded*** the document containing Class Members' PII, Plaintiffs' standing is simply not disrupted by *TransUnion*. To the extent there is doubt about the impact of *TransUnion*, the Court should continue to treat *McMorris* as good law unless and until otherwise established by the Second Circuit or the Supreme Court. *Bonobos*, 2022 WL 170622, at *3, n.1.

III. CONCLUSION

For the reasons set forth above and in Plaintiffs' opposition to Defendant's motion to dismiss (Dkt. No. 54), Plaintiffs respectfully request that the Court rely on, or reaffirm, its prior finding of standing and grant preliminary approval of the Settlement.

Dated: May 12, 2022

Respectfully submitted,

/s/ *William B. Federman*
William B. Federman
(S.D. New York #WF9124)
A. Brooke Murphy
(admitted *pro hac vice*)
FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com
abm@federmanlaw.com

Interim Lead Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that on May 12, 2022, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ *William B. Federman*
William B. Federman