UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|---|---|---|
| IN RE CHRISTIE'S DATA BREACH LITIGATION, | : | 24-CV-4221 (JMF) |
| *This Document Relates To:* *All Member Cases* | : | MEMORANDUM OPINION AND ORDER |

JESSE M. FURMAN, United States District Judge:

In this case, familiarity with which is presumed, a group of consumers filed a class action alleging that their personal information — including drivers' license numbers and passport numbers — was disclosed in a 2024 hacking incident targeting Defendant Christie's Inc.'s computer systems. *See* ECF No. 43, ¶¶ 22-24. On December 13, 2024, the parties filed a motion for preliminary approval of a class action settlement. *See* ECF No. 49. On December 18, 2024, the Court issued an order directing the parties to file supplemental briefs addressing, among other things, whether Plaintiffs have standing. *See* ECF Nos. 50, 45. The parties subsequently filed briefs arguing that the Court should approve the settlement. *See* ECF Nos. 51-54.

Upon review of the parties' filings and relevant cases, the Court is inclined to believe that Plaintiffs' standing may turn on whether they satisfy the third factor in *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021), namely "whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud," *id.* at 303. Specifically, courts appear to be divided on the question of whether the exposure of drivers' license numbers satisfies this inquiry. *Compare, e.g.*, *Rand v. Travelers Indem. Co.*, 637 F. Supp. 3d 55 (S.D.N.Y. 2022) (agreeing that "a driver's license number . . . can be used to" commit various types of fraud), *with Cantinieri v. Verisk Analytics, Inc.*, No. 21-CV-6911 (NJC) (JMW), 2024 WL 5202579, at *17 (E.D.N.Y. Dec. 23, 2024) (concluding plaintiff "ha[d] not established that the disclosure of her driver's license number . . . would be likely to subject [her] to a perpetual risk of identity theft or

fraud"). In many instances, however, the answer appears to turn on whether there are allegations in the record that (1) fraudulent activity has already resulted from the exposure of drivers' license numbers or (2) fraudulent activity could result from the combined exposure of drivers' license numbers with the other exposed information. *See, e.g.*, *In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 466–67 (S.D.N.Y. 2022) (distinguishing cases that "did not involve well-pleaded allegations of actual proof of identity theft as a result of the disclosure" of DLNs); *Cantinieri*, 2024 WL 5202579, at *17 (distinguishing *In re USAA Data Securities Litigation* because the complaint "lack[ed] allegations that the disclosure of a driver's license number, name, address, and birthdate, [could] provide an opening for fraud" (internal quotations marks omitted)); *see also Stallone v. Farmers Grp., Inc.*, No. 221-CV-01659 (GMN) (VCF), 2022 WL 10091489, at *5 (D. Nev. Oct. 15, 2022) ("Plaintiff cites to multiple experts for the proposition that the PII stolen can, and will likely, be used to [commit fraud].").

In light of the foregoing, and mindful of the fact that the Court may consider materials outside the pleadings in assessing whether Plaintiffs have standing, *see, e.g.*, *Tandon v. Captain's Cove Marina of Bridgeport, Inc.*, 752 F.3d 239, 243 (2d Cir. 2014), Plaintiffs shall, **no later than February 4, 2025**, either file (1) a declaration addressing the potential for fraud or identity theft resulting from the information exposed in the 2024 data breach, including but not limited to drivers' license numbers and passport numbers; or (2) a supplemental brief, **not to exceed five pages**, addressing why such a declaration should not be required. Defendant may file a response, in the form of a supplemental brief **not to exceed five pages**, by **February 7, 2025**.

SO ORDERED.

Dated: January 28, 2025
New York, New York

JESSE M. FURMAN
United States District Judge