

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 08/11/2023

-----X
BRUCE YUILLE,

Plaintiff,

-v-

UPHOLD HQ INC.,

Defendant.
-----X

22-cv-7453 (LJL)

OPINION AND ORDER

LEWIS J. LIMAN, United States District Judge:

Defendant Uphold HQ Inc. (“Defendant” or “Uphold”) moves, pursuant to Federal Rule of Civil Procedure 12(b)(6), to dismiss the first, second, third, fourth, sixth, and seventh causes of action of the complaint of plaintiff Bruce Yuille (“Plaintiff” or “Yuille”) for failure to state a claim upon which relief can be granted. Dkt. No. 18. For the following reasons, the partial motion to dismiss is granted in part and denied in part.

BACKGROUND

For purposes of this motion, the Court accepts as true the well-pleaded allegations of the complaint, Dkt. No. 3 (“Complaint” or “Compl.”), as supplemented by the documents incorporated by reference.

Plaintiff is a 77-year-old retired individual who lives in Clarkston, Oakland County, Michigan. *Id.* ¶¶ 9, 22. Uphold is a “cryptocurrency exchange and digital money platform” that allows its 1.7 million customers to transfer, purchase, trade, hold, and sell cryptocurrency, equities, precious metals, and fiat currency. *Id.* ¶¶ 2, 9, 15, 75. Uphold permits its users to convert and process transactions between these various asset classes, offering a “unique ‘Anything -to-Anything’ trading experience.” *Id.* ¶ 16 (citation omitted). Uphold, whose

principal place of business is New York, New York, has processed nearly \$6 billion in transactions since its inception. *Id.* ¶¶ 2, 9, 72.

The allegations in the Complaint focus on an account that Yuille opened at Uphold in August 2021. *Id.* ¶¶ 22, 24. In or around July 2021, Yuille began to look for a secure cryptocurrency exchange to hold his Bitcoin assets. *Id.* ¶ 21. The Complaint alleges that Yuille was drawn to Uphold’s account in large part because of Uphold’s focus on security. *See id.*

¶¶ 21, 23. Uphold has also made several representations about its efforts to safeguard customer accounts. On its website, Uphold asserts that “[s]ecurity is in our DNA. Our number one priority is to protect you, your money, and your information. Security is built into our systems and culture.” *Id.* ¶¶ 3, 19 (citation omitted). Additionally, Plaintiff alleges that Uphold has made the following representations related to its account security.

- “[O]ur Information Security and Personal Information protection programs . . . are designed to meet or exceed regulatory requirements, establish the highest levels of trust with our members, and prevent bad actors from taking advantage of our systems, members, employees, or brand.”
- “We deploy layered defenses to limit the scope and depth of potential attacks, as well as sophisticated encryption.”
- “Security professionals routinely conduct security audits and penetration testing of our systems.”
- “Bug Bounty Program - to encourage reporting of security vulnerabilities on the platform.”
- “The Uphold Security Operations Centre monitors systems year-round and ***responds immediately*** to any detected threat.”
- “All our providers undergo appropriate due diligence checks. Special attention is paid to integrations incorporating sensitive data.”
- “The Uphold team are background checked by an accredited vendor. Mandatory security and privacy training is conducted regularly.”
- “We’ll [] do email verification if we detect anything untoward. If we detect unusual activity, we’ll send you an email to verify it is you.”

- “Uphold is a pioneer in our space when it comes to the security of our consumers: we are one of the first companies working with digital currencies to become certified to PCI/DSS [the Payment Card Industry Security Standards Council], one of the most stringent security standards in the industry. Being compliant means that we are doing our very best to keep our members’ valuable information secure and out of the hands of people who could use that data in a fraudulent way.”

Id. ¶ 20 (emphasis in original) (cleaned up). Yuille chose to open an account (the “Account”) with Uphold and have his Bitcoin transferred into the account “because of [Uphold’s] representations of account security, superlative customer service, [its] purported secure multifactor authentication, and the fact that Uphold claimed to monitor its platform for security threats 24 hours a day and every day of the year.” *Id.* ¶ 21; *see also id.* ¶ 23 (“Yuille trusted and relied on Uphold’s representations that his assets would be safe with Uphold.”). According to Yuille’s representations to Uphold on August 23, 2021, the purposes of the Account were (1) “to hold BTC,” (2) “to sell [BTC] and reduce [BTC] to dollars and transfer dollars to his bank,” and (3) “to trade crypto coins like those listed on Uphold.” *Id.* ¶ 7. In August 2021, Yuille deposited 106 Bitcoin into the Account. *Id.* ¶ 24.

Uphold allegedly did not live up to its representations about its security; within four months of the date when Yuille opened the Account, unauthorized users siphoned approximately 100 Bitcoin from the Account, worth roughly \$5 million at the time. *Id.* ¶¶ 1, 45, 54. The events in question began on December 7, 2021 at 8:01 p.m., when a third party based in Nigeria attempted to log into the Account. *Id.* ¶ 47. That attempt failed, but between December 7 and December 9, an unauthorized third party tried and failed to change the password associated with Yuille’s Account on five separate occasions. *Id.* ¶¶ 46–47. On December 9, 2021 at 10:48 a.m., an unauthorized party successfully took over Yuille’s Account, without Yuille’s permission or knowledge, changing his password and then eight minutes later, changing the e-mail associated with the Account. *Id.* ¶¶ 48–49. The Complaint also alleges that Uphold may have permitted the

two-factor authentication of the Account to be turned off, modified, or accessed without Yuille's permission. *Id.* ¶ 33.

That same day, Yuille attempted to log into his account on three separate occasions but was unable to do so. *Id.* ¶ 50. At 4:41 p.m., Yuille sent an email to Uphold indicating that he was locked out of his account, which he had previously used on December 7 to sell 0.5 Bitcoin and that he was unable to reset his password despite trying three times. *Id.* ¶ 51. Yuille requested Uphold's help. *Id.* Uphold's customer service representative responded, not by recognizing that Yuille's Account had been hacked and freezing the Account, but by recommending that Yuille check his spam folder for the password verification emails. *Id.* ¶ 52. Beginning approximately eight hours after Yuille emailed Uphold and continuing until 5:00 p.m. on December 11, 2021, approximately \$5 million of Bitcoin was transferred out of the Account. *Id.* ¶ 54. The Complaint alleges that had Uphold locked and restricted access or transfers out of Yuille's account, Yuille would still have access to his Bitcoin. *Id.* ¶ 56.

The Complaint also alleges that Uphold was on notice of the risk of cyberattacks, hacking, and improper transfers and did not adequately address these risks. *Id.* ¶ 26. The Complaint cites to Uphold's website, where Uphold acknowledged that there was an increase of fifty times in the activity of "scammers and bad actors" and that its customer service was inadequate to deal with the threats. *Id.* ¶¶ 28–29. To address this increased activity, Uphold took various steps to improve its customer service response times, including decreasing the number of situations in which Uphold would restrict access to customers' accounts by almost 50%, permitting individuals to change an email address and two-factor authentication through their account instead of through a customer service specialist, and permitting customers to correct account information without risk of account restriction. *Id.* ¶ 30. These measures may

have improved Uphold’s customer service response times, but they weakened its account security by reducing the situations in which Uphold would restrict account access and increasing the ability of customers to make changes without the support of customer service. *Id.* ¶ 32.

Plaintiff alleges that Uphold has a duty to protect its customers’ assets and to protect accounts on its platform, but that Uphold failed to discharge its duties, resulting in the withdrawal of \$5 million of Bitcoin from the Account without Yuille’s authorization. *Id.* ¶ 57. Specifically, the Complaint alleges that “Uphold failed to provide reasonable and appropriate security to prevent unauthorized access to its customer’s account and [Bitcoin] wallet, and the assets stored therein” by, among other things, (1) misrepresenting “the safety and security of” its accounts; (2) failing “to adequately safeguard and protect” the accounts; (3) failing “to use readily available security measures to prevent or limit unauthorized access to customer accounts and to prevent unauthorized transactions from occurring on those accounts”; (4) failing “to suspend user credential after a certain number of unsuccessful access attempts”; (5) lacking appropriate monitoring solutions and failing to monitor accounts for unauthorized access that would have enabled Uphold to detect the intrusion in the Account; (6) failing “to implement defenses to identify unauthorized third parties such as delaying transfers from accounts on which the password was recently changed or simply delaying transfers from accounts to allow for additional verifications from customers”; (7) failing “to implement reasonable means for customers to contact Uphold without undue delay after discovering account security issues”; (8) failing “to promptly act after being notified by a customer that they cannot access their account or suspect an account has been compromised, including by timely locking the account, restricting access to the account, or restricting transfers from the account until the account is secured”; and (9) failing “to act reasonably and adequately—by timely locking the account,

restricting access to the account, or restricting transfers from the account until the account was secured—after being notified that a customer could not access their account or suspected their account had been compromised.” *Id.* ¶¶ 58–59.

The Complaint also alleges that Uphold did not fulfill its obligations under the Electronic Fund Transfer Act (“EFTA”), 15 U.S.C. § 1693 *et seq.* and its implementing regulations, 12 C.F.R. § 1005.1 *et seq.* (“Regulation E”). Plaintiff alleges that, as defined in the EFTA, Uphold is a financial institution, Yuille is a consumer, the Account was established for personal, family, or household purposes, and the transactions at issue were electronic fund transfers (“EFT”) and unauthorized. *Id.* ¶ 44. Under the EFTA and Regulation E, Plaintiff alleges that Uphold was required to provide various initial disclosures, including a summary of the consumer’s rights. *Id.* ¶ 39. Further, after a financial institution receives an oral or written notice of an unauthorized funds transfer, the institution must conduct an investigation, complete the investigation within ten business days, and correct any error that it determines was committed within one business day of determining that the error had occurred, including by either correcting the error or provisionally recrediting the account while the investigation is ongoing. *Id.* ¶¶ 40–41. However, Plaintiff alleges that Uphold took none of these required actions. *Id.* ¶¶ 34, 43, 64–66.

Based on these allegations, the Complaint asserts seven causes of action against Defendant. (1) violation of the EFTA and Regulation E (“Count I”), *id.* ¶¶ 67–73; (2) violation of New York General Business Law (“NYGBL”) § 349 (“Count II”), *id.* ¶¶ 74–81; (3) violation of the Michigan Consumer Protection Act (“MCPA”), Mich. Comp. Laws Ann. § 445.901 *et seq.* (“Count III”), *id.* ¶¶ 82–86; (4) intentional misrepresentation (“Count IV”), *id.* ¶¶ 87–94; (5) negligence (“Count V”), *id.* ¶¶ 95–107; (6) gross negligence (“Count VI”), *id.* ¶¶ 108–14; and

(7) a declaratory judgment under 28 U.S.C. § 2201 that Section 12.4 of Uphold’s General Terms and Conditions (“Terms and Conditions”), which limits Uphold’s liability to the actual fees paid by a customer in the preceding three months or \$100, is unenforceable (“Count VII”), *id.* ¶¶ 115–18. Plaintiff seeks, *inter alia*, compensatory damages, treble damages under the EFTA and NYGBL § 349, a declaratory judgment, and attorneys’ fees under the EFTA, NYGBL § 349, and Mich. Comp. Laws Ann. § 445.901. *Id.* ¶ 119.

PROCEDURAL HISTORY

Plaintiff filed his Complaint on August 31, 2022. Dkt. No. 1. On December 12, 2022, Defendant filed a motion to dismiss Counts I, II, III, IV, VI, VII of the Complaint, along with a supporting memorandum of law and declaration. Dkt. Nos. 18–20. On January 12, 2023, Plaintiff filed a memorandum of law in opposition to the motion to dismiss, Dkt. No. 23, to which Defendant replied and submitted another supporting declaration on January 26, 2023, Dkt. Nos. 26–27.¹ On June 9, 2023, the Court permitted the parties to submit supplemental briefing addressed solely to the question whether the EFTA and Regulation E apply to cryptocurrency transactions.² Dkt. No. 47. Both parties submitted supplemental letter briefs on June 16, 2023. Dkt. Nos. 48–49.

¹ On May 30, 2023, Defendant requested pursuant to Rule 13(b)(3) of the Rules for the Division of Business Among District Judges, Southern District of New York, that the Court deem this action related to *Nero, et al. v. Uphold HQ Inc., et al.*, 22-cv-01602 (S.D.N.Y.), an earlier-filed action pending before the Hon. Denise L. Cote, and refer the question of whether the two cases should be consolidated to Judge Cote, Dkt. No. 43, a request that Plaintiff opposed, Dkt. No. 44. The Court denied that request on June 9, 2023. Dkt. No. 46.

² On March 21, 2023, Defendant filed a letter brief addressing Judge Cote’s decision in *Rider v. Uphold HQ Inc.*, 2023 WL 2163208, at *2–3 (S.D.N.Y. Feb. 22, 2023), which found that the EFTA and Regulation E applied to electronic transfers of cryptocurrency. Dkt. No. 39. Plaintiff responded to Defendant’s letter on March 27, 2023. Dkt. No. 40. Because the parties did not have permission to file these supplemental letter briefs, neither filing will be considered by the Court on this motion.

LEGAL STANDARD

To survive a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted, a complaint must include “sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’”

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A complaint must offer more than “labels and conclusions,” “a formulaic recitation of the elements of a cause of action,” or “naked assertion[s]” devoid of “further factual enhancement.” *Twombly*, 550 U.S. at 555, 557. The ultimate question is whether “[a] claim has facial plausibility, [*i.e.*,] the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. “Determining whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Id.* at 679. Put another way, the plausibility requirement “calls for enough fact to raise a reasonable expectation that discovery will reveal evidence [supporting the claim].” *Twombly*, 550 U.S. at 556; *see also Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 46 (2011).

DISCUSSION

Uphold argues that each of Plaintiff’s claims, except for his negligence claim, must fail as a matter of law. Yuille counters that the “Complaint contains detailed, factual allegations to support each of Yuille’s claims.” Dkt. No. 23 at 1–2. The Court addresses each of Uphold’s arguments in turn.

I. Count I: EFTA

The EFTA provides a “basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems,” to protect

“individual consumer rights.”³ 15 U.S.C. § 1693(b). The EFTA, *inter alia*, sets forth disclosure obligations for the terms and conditions of electronic fund transfers, *id.* § 1693c(a), requires a financial institution to share documentation of the electronic fund transfer with the consumer, *id.* § 1693d, and imposes obligations on financial institutions to expeditiously investigate and correct errors, including unauthorized electronic fund transfers. *id.* § 1693f. If a financial institution fails to “provisionally recredit a consumer’s account within” ten days and either does “not make a good faith investigation of the alleged error” or “did not have a reasonable basis for believing that the consumer’s account was not in error,” then the consumer is entitled to three times her actual damage sustained in connection with the financial institution’s failure to comply with Section 1693f. *See id.* §§ 1692f, 1692m(a)(1). The EFTA grants authority to the Consumer Financial Protection Bureau (“CFPB”) to “prescribe regulations to carry out the purposes” of the EFTA. *Id.* § 1693b(a). These regulations apply to “any electronic fund transfer that authorizes a financial institution to debit or credit a consumer’s account.” 12 C.F.R. § 1005.3(a).

The parties spar over whether the EFTA can categorically reach cryptocurrency transactions. The text of the EFTA does not expressly address its applicability to cryptocurrency transactions. Cryptocurrency did not exist when Congress passed the EFTA in 1978. That cryptocurrency did not exist when the EFTA was passed, however, cannot, standing alone, limit the EFTA’s application to cryptocurrency. *See Am. Broad. Companies, Inc. v. Aereo, Inc.*, 573 U.S. 431, 449 (2014) (suggesting that old statutes—including the Copyright Act of 1976—can apply to “new technologies,” but that “courts often apply a statute’s highly general language in light of the statute’s basic purposes”). And, though Congress has amended the EFTA since

³ A “consumer” is defined as “a natural person” under the EFTA. 15 U.S.C. § 1693a(6); *see also* 15 C.F.R. § 1005.2(e).

cryptocurrency’s inception, *see* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, 2081 (July 21, 2010) (noting that the title of Section 1084 is “Amendments to the Electronic Fund Transfer Act”), it did not incorporate provisions explicitly related to cryptocurrency transfers. This fact too is not dispositive—or even persuasive—with respect to the analysis of whether the EFTA applies to cryptocurrency. *See Bostock v. Clayton Cnty.*, 140 S. Ct. 1731, 1747 (2020) (discussing the difficulty of inferring statutory meaning from congressional inaction because “[t]here’s no authoritative evidence explaining why later Congresses” decided not to act. “All we can know for certain is that speculation about why a later Congress declined to adopt new legislation offers a ‘particularly dangerous’ basis on which to rest an interpretation of an existing law a different and earlier Congress did adopt.”); *see also Pension Ben. Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990) (“Congressional inaction lacks ‘persuasive significance’ because ‘several equally tenable inferences’ may be drawn from such inaction, ‘including the inference that the existing legislation already incorporated the offered change.’” (citation omitted)). The parties thus focus their argument on the definition of “electronic fund transfer.” *See* Dkt. No. 48 at 2–4; Dkt. No. 49 at 1–2.

An “electronic fund transfer” is defined in the EFTA and Regulation E as “any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account.” *Id.* § 1693a(7); *see also* 12 C.F.R. § 1005.3(b). This definition only goes so far: It does not define “funds” and thus does not directly clarify whether the phrase “any transfer of funds” includes cryptocurrency transactions. The statute does provide a non-exclusive list of examples of electronic fund transfers, including “point-of-sale transfers, automated teller machine

transactions, direct deposits or withdrawals of funds, and transfers initiated by telephone.”

15 U.S.C. § 1693a(7). It also excludes certain transactions:

(A) any check guarantee or authorization service which does not directly result in a debit or credit to a consumer’s account; (B) any transfer of funds [for a consumer within a system that is] not designed primarily to transfer funds on behalf of a consumer; (C) any transaction the primary purpose of which is the purchase or sale of securities or commodities through a broker-dealer registered with or regulated by the Securities and Exchange Commission; (D) [any intra-institutional] automatic transfer . . . pursuant to an agreement between a consumer and a financial institution . . . ; or (E) any transfer of funds which is initiated by a telephone conversation between a consumer and an officer or employee of a financial institution.

Id. § 1693a(7)(A)–(E). Uphold argues that “what all of these statutory examples have in common is that they are denominated in U.S. Dollars” and thus, the EFTA “was intended to apply only to electronic transfers of fiat currency . . . and not transactions in cryptocurrency.”

Dkt. No. 49 at 1–2. Plaintiff counters that the term “funds” is broad enough to encompass liquid assets generally, and thus the EFTA applies to Bitcoin transactions. Dkt. No. 48 at 3.

The only case to squarely address whether the EFTA applies to cryptocurrency transfers—and whether the term “funds” includes cryptocurrency—is from this District, *Rider v. Uphold HQ Inc.*, 2023 WL 2163208 (S.D.N.Y. Feb. 22, 2023). There, the Honorable Denise L. Cote considered the defendants’ motion to dismiss a complaint brought on behalf of a putative class that claimed that Uphold failed to correctly implement security protections for its customers. *Id.* at *1. Specifically, the defendants moved to dismiss the plaintiffs’ claim under the EFTA, arguing that cryptocurrency does not constitute “funds” within the meaning of the EFTA. *Id.* at *2. Because the EFTA does not define the term “funds,” Judge Cote looked to Black’s Law Dictionary for the term’s ordinary meaning. Black’s Law Dictionary defines “funds” as a “[a] sum of money or other liquid assets established for a specific purpose.” *Id.* at *3 (quoting *Funds*, Black’s Law Dictionary (11th ed. 2019)). The court also noted that Black’s

Law Dictionary defines “cryptocurrency” as “[a] digital or virtual currency that is not issued by any central authority, is designed to function as a medium of exchange, and uses encryption technology to regulate the generation of units of currency, to verify fund transfers, and to prevent counterfeiting.” *Id.* (quoting *Cryptocurrency*, Black’s Law Dictionary). The court also analyzed how other courts have interpreted the term “funds” in the federal money laundering statute. *See* 18 U.S.C. § 1956. The court rejected the defendants’ arguments and concluded that “[u]nder its ordinary meaning, the term ‘cryptocurrency’ means a digital form of liquid, monetary assets that constitute ‘funds’ under the EFTA.” *Rider*, 2023 WL 2163208, at *3 (first citing *United States v. Iossifov*, 45 F.4th 899, 913 (6th Cir. 2022), and then citing *United States v. Day*, 700 F.3d 713, 725 (4th Cir. 2012)). The court also rejected the defendants’ argument that the CFPB, in its November 22, 2016 statement, excluded cryptocurrency from the ambit of the term “funds” under the EFTA because the CFPB “expressly stated that it was taking no position with respect to the application of existing statutes, like the EFTA, to virtual currencies and services.” *Rider*, 2023 WL 2163208, at *3.

Plaintiff argues that the Court should adopt Judge Cote’s interpretation of the word “funds,” *see* Dkt. No. 48 at 3, while Defendant argues that it should reject her understanding of the term, *see* Dkt. No. 49 at 1–2, 1 n.1.⁴ The Court, however, need not determine whether the term “funds” as used in the definition of electronic fund transfer includes cryptocurrency transfers—and thus, more generally, whether an “electronic fund transfer” can include a transfer of Bitcoin—because the Court finds that the Account is not an “account” within the meaning of

⁴ The definition of “account” is also relevant to whether Uphold is a “financial institution,” which is defined as “a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly, *holds an account belonging to a consumer.*” 15 U.S.C. § 1693a(9) (emphasis added); *see also* 15 C.F.R. § 1005.2(i).

the EFTA. The EFTA defines an “account” as “a demand deposit, savings deposit, or other asset account . . . *established primarily for personal, family, or household purposes*,” 15 U.S.C. § 1693a(2) (emphasis added); 15 C.F.R. § 1005.2(b)(1).

The EFTA does not explicitly set the boundaries of what constitutes “personal, family, or household purposes.” Some accounts are clearly excluded from the reaches of the EFTA. For example, an Interest on Lawyer’s Account (“IOLA”) does not fall under the provisions of the EFTA because an IOLA is “by definition . . . an account that is established purely for commercial reasons.” *Fischer & Mandell LLP v. Citibank, N.A.*, 2009 WL 1767621, at *3–4 (S.D.N.Y. June 22, 2009) (Sullivan, J.) (holding that “the EFTA does not apply to accounts that are used primarily or solely for commercial purposes.”); *see also Regatos v. N. Fork Bank*, 257 F. Supp. 2d 632, 638 (S.D.N.Y. 2003) (holding that “the EFTA [is] inapplicable” to an account that “was purely commercial”). In contrast, a checking account opened for the purposes of received direct deposits from a consumer’s employer and to pay for personal and household items like rent, utilities, and groceries would clearly fall under the auspices of the EFTA. Between these two extremes, however, there can be uncertainty as to whether an account was established for personal, family, or household purposes.

To give meaning to the phrase, courts have looked to interpretations of the identical phrase in the Truth in Lending Act, 15 U.S.C. § 1601 *et seq.* (“TILA”), which, *inter alia*, governs “consumer” credit. “Consumer,” when used as an adjective in the TILA in “reference to a credit transaction . . . characterizes the . . . the money, property, or services which are the subject of the transaction [as] primarily for personal, family, or household purposes.” 15 U.S.C. § 1602(i). The EFTA and TILA were both passed as part of the Consumer Credit Protection Act of 1968 (“CCPA”) and share a “common purpose . . . to protect consumers with respect to

financial credit.” *Clemmer v. Key Bank Nat. Ass’n*, 539 F.3d 349, 353 (6th Cir. 2008). Because both the EFTA and TILA use the phrase “primarily for personal, family, or household purposes” to define an account and consumer credit, respectively, courts interpreting whether an “account” falls under the provisions of the EFTA have looked to how other courts have interpreted the phrase in reference to the TILA, where the phrase has received significantly more attention. *See Cobb v. Monarch Fin. Corp.*, 913 F. Supp. 1164, 1174 (N.D. Ill. 1995) (“Under the TILA, like the EFTA, the term ‘personal, family, or household purposes’ distinguishes ‘consumer’ transactions from ‘business’ transactions.” (citing *American Express Co. v. Koerner*, 452 U.S. 233, 242–43 (1981))); *see also Atl. Cleaners & Dyers v. United States*, 286 U.S. 427, 433 (1932) (noting that although “not rigid,” there is a “natural presumption that identical words used in different parts of the same act are intended to have the same meaning”);⁵ *Johnson v. W. Suburban Bank*, 225 F.3d 366, 379 (3d Cir. 2000) (holding, in reference to the EFTA and TILA’s class action language that was added to the EFTA by the 1978 amendment and the TILA by the 1974 and 1976 amendments, that “[w]e do not believe that Congress would have different intended meanings for identical statutory language contained in similar statutes”). There may also be occasion to look to how courts have given meaning to the definition of “consumer debt” under the Bankruptcy Code—defined as “debt incurred by an individual primarily for a personal, family, or household purpose,” 11 U.S.C. § 101(8)—because “Congress adapted the Bankruptcy Code’s definition of “consumer debt” from the consumer protection laws—in particular the

⁵ The Supreme Court has held that this presumption “yields readily to indications that the same phrase used in different parts of the same statute means different things, particularly where the phrase is one that speakers can easily use in different ways without risk of confusion.” *Barber v. Thomas*, 560 U.S. 474, 484 (2010). Here, there is no indication that the phrase “personal, family, or household purposes” as used in different parts of the CCPA were intended to mean different things. Nor is “personal, family, or household purposes” the kind of phrase that “speakers can easily use in different ways without risk of confusion.” *Id.*

[TILA] . . . , which contains a similar definition.” *In re Cherrett*, 873 F.3d 1060, 1072 (9th Cir. 2017).

Though “[t]he Second Circuit has not articulated a standard for determining whether a loan is obtained for personal or business purposes under TILA,” “[m]ost other courts that have addressed the issue have held that a court must look at the entire transaction and surrounding circumstances to determine a borrower's primary motive.” *Mauro v. Countrywide Home Loans, Inc.*, 727 F. Supp. 2d 145, 153 (E.D.N.Y. 2010) (Bianco, J.) (collecting cases). “As a general matter, when a party obtains a loan in order to make a profit, that loan is not considered a ‘personal’ loan under TILA.” *Id.*; see also *Matter of Booth*, 858 F.2d 1051, 1054–55 (5th Cir. 1988) (“Cases decided under the Truth in Lending Act indicate that when the credit transaction involves a profit motive, it is outside the definition of consumer credit.” (collecting cases)). Similarly, in the bankruptcy context, “a debt that ‘was not incurred with a profit motive or in connection with a business transaction . . . is considered ‘consumer debt’ for purposes of [the Bankruptcy Code].” *Curtis v. Propel Prop. Tax Funding, LLC*, 915 F.3d 234, 245–46 (4th Cir. 2019) (alteration in original) (quoting *In re Kestell*, 99 F.3d 146, 149 (4th Cir. 1996)); see also *In re Cherrett*, 873 F.3d at 1067 (“We have held that ‘[d]ebt incurred for business ventures or other profit-seeking activities is plainly not consumer debt.’” (citation omitted)); *In re Grullon*, 2014 WL 2109924, at *5 (Bankr. S.D.N.Y. May 20, 2014) (“In determining whether a debt is a consumer debt, courts have considered whether it was incurred with a profit motive.”).

Thus, the relevant question here is whether the Account was “established primarily” for profit-making purposes. See *Frey v. First Nat. Bank Sw.*, 602 F. App’x 164, 169 (5th Cir. 2015) (The EFTA “asks only for what [purpose] the account was established” (citation omitted)). The Complaint indicates that the Account was primarily established for profit-making purposes. The

Complaint alleges that Plaintiff opened the Account for three “purpose[s]”: (1) “to hold [Bitcoin]”; (2) “to sell and reduce to dollars and transfer dollars to his bank”; and (3) “to trade crypto coins like those listed on Uphold.”⁶ Compl. ¶ 22. The purpose for which the Account was established was for investment, which has an inherent profit motive. Notably, Yuille does not allege that the Account had any of the indicia an account established for “personal, family, or household purposes”: He did not establish the Account to “receive[] direct deposits from [his] paychecks,” *Cobb*, 913 F. Supp. at 1175, and he did not establish or maintain the account to hold funds earmarked to pay household or other personal expenses. Instead, Plaintiff alleges that he had to “reduce” his holdings in the Account “to dollars and transfer dollars to his bank,” presumably to use those dollars for personal expenses. Compl. ¶ 22.

The Court draws support for this conclusion from the distinction that has emerged between loans entered into for primary residences, which generally are considered consumer debt under TILA and the bankruptcy code, and those that are entered into for rental properties, which are not. *See Mauro*, 727 F. Supp. 2d at 154 (collecting cases) (holding that “it is well settled that a loan obtained in order to invest in non-owner occupied rental properties is a loan for business purposes” and suggesting that a loan used for a personal residence would fall under the auspices of TILA). *But see In re Cherrett*, 873 F.3d at 1063–64, 1066–67 (in bankruptcy context, holding that “a debt incurred to purchase a personal residence is” not “a consumer debt as a matter of law” and that the loan in question, although used to purchase a personal residence was not “consumer debt” because it had the primary business purpose of encouraging debtor to leave a prior job in order to further his carrier). The fact that an individual may ultimately use

⁶ Plaintiff’s conclusory allegation that “Yuille’s accounts were accounts established for personal, family, or household purposes,” Compl. ¶ 44, unsupported by facts to that effect, is insufficient to state a claim under the EFTA.

the proceeds from the rental property for personal purposes appears irrelevant to the analysis under TILA. Thus, even if the Complaint can be read to suggest that Plaintiff transferred money from the Account to a bank account that was used for personal and household purposes, the Account itself was established for investment purposes and the derivative use of the investment income does not change that conclusion.

The Court also draws support for its conclusion from the Federal Reserve Board's Official Staff Interpretation of Regulation E and its definition of the word "account." *See Vincent v. The Money Store*, 736 F.3d 88, 106 (2d Cir. 2013) (noting that "the Official Staff Commentary promulgated by the [CFPB] as an interpretation of Regulation Z may warrant deference as a general matter." (alteration omitted) (quoting *Chase Bank USA, N.A. v. McCoy*, 562 U.S. 195, 211 (2011))).⁷ The Official Staff Interpretation to 12 C.F.R. § 1005.2(2)(b), which defines the term "Account" for the purposes of Regulation E lists as an "[e]xample[] of accounts not covered by Regulation E" "[a]ccounts for accumulating funds to purchase U.S. savings bonds." 12 C.F.R. Pt. 1005, Supp. I, ¶ 2.iii of commentary to 12 C.F.R. § 1005.2(2)(b). This commentary suggests that accounts established for investment purposes (to purchase U.S. savings bonds) are not established for "personal, family, or household purposes" such that the EFTA would apply.

Accordingly, because Plaintiff has not pled that the Account is an "account" under the EFTA, his EFTA claim must fail.⁸

⁷ Although specific to Regulation Z and the TILA, there is no reason why these holdings would not also apply to the CFPB's commentary to Regulation E and the EFTA.

⁸ The definition of "electronic fund transfer" contains an exception for "any transaction the primary purpose of which is the purchase or sale of securities or commodities through a broker-dealer registered with or regulated by the Securities and Exchange Commission." 15 U.S.C. § 1693a(7)(C). Because Uphold is not a registered broker-dealer, and cryptocurrencies (for the time being) are not securities or commodities regulated by the Securities and Exchange

II. Count II: Violation of NYGBL § 349

Section 349 of the NYGBL (“Section 349”) “makes unlawful ‘[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in [New York] state,’” *Pelman ex rel. Pelman v. McDonald’s Corp.*, 396 F.3d 508, 511 (2d Cir. 2005) (first alteration in original) (quoting NYGBL § 349), and “provides a private right of action to ‘any person who has been injured by reason of any violation of th[e] section,’” *Kacocha v. Nestle Purina Petcare Co.*, 2016 WL 4367991, at *13 (S.D.N.Y. Aug. 12, 2016) (quoting NYGBL § 349(h)). “To state a claim under § 349, a plaintiff must allege: (1) the act or practice was consumer-oriented; (2) the act or practice was misleading in a material respect; and (3) the plaintiff was injured as a result.” *Spagnola v. Chubb Corp.*, 574 F.3d 64, 74 (2d Cir. 2009); *see also Goshen v. Mut. Life Ins. Co. of New York*, 774 N.E.2d 1190, 1195 (N.Y. 2002) (“Under General Business Law § 349(h) “[a] prima facie case requires . . . a showing that defendant is engaging in an act or practice that is deceptive or misleading in a material way and that plaintiff has been injured by reason thereof” (citation omitted)). A plaintiff is “not required to meet the heightened pleading requirements of Federal Rule of Civil Procedure 9(b) for [his] claims.” *Lugones v. Pete & Gerry’s Organic, LLC*, 440 F. Supp. 3d 226, 240 (S.D.N.Y. 2020). Defendant does not contest that its practices were consumer oriented or that Plaintiff was injured

Commission or the Commodities Futures Trading Commission, *see* 12 C.F.R. 1005.3 (expanding the list of exclusions from the definition of “electronic fund transfer” to include regulated securities and commodities), Plaintiff suggests that the fraudulent transactions are governed by the EFTA. *See* Dkt. No. 48 at 2–3. The Court notes that the primary purpose for which an account is established may differ from the primary purpose for which an electronic fund transfer is initiated. Because the Account is not an “account” for the purposes of the EFTA, the purpose for which the fraudulent transfers were initiated cannot bring the transfers under the auspices of the EFTA.

as a result;⁹ rather, Defendant argues that Plaintiff has not adequately alleged that the act or practice was misleading. *See* Dkt. No. 20 at 7–8.

In order to state a claim under Section 349, a plaintiff must plead that the defendant’s statements were “likely to mislead a reasonable consumer acting reasonably under the circumstances.” *Michelo v. Nat’l Collegiate Student Loan Tr.* 2007-2, 419 F. Supp. 3d 668, 701 (S.D.N.Y. 2019) (quoting *Oswego Laborers’ Loc. 214 Pension Fund v. Marine Midland Bank, N.A.*, 647 N.E.2d 741, 745 (N.Y. 1995)); *see also Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (“As for the ‘materially misleading’ prong, ‘[t]he New York Court of Appeals has adopted an objective definition of “misleading,” under which the alleged act must be “likely to mislead a reasonable consumer acting reasonably under the circumstances.”’”) (quoting *Cohen v. JP Morgan Chase & Co.*, 498 F.3d 111, 126 (2d Cir. 2007))). A misrepresentation can come in the form of an affirmative misrepresentation or a materially deceptive omission. *See Fishon v. Peloton Interactive, Inc.*, 620 F. Supp. 3d 80, 98–105 (S.D.N.Y. 2022). Puffery—“defined as exaggerated general statements that make no specific claims on which consumers could rely,” *Pelman v. McDonald’s Corp.*, 237 F. Supp. 2d 512, 528 n.14 (S.D.N.Y. 2003), because they are “subjective claims about products, which cannot be proven either true or false,” *Time Warner Cable, Inc. v. DIRECTV, Inc.*, 497 F.3d 144, 159 (2d Cir. 2007)—however, is not actionable under Section 349, *see In re Scotts EZ Seed Litig.*, 2013 WL 2303727, at *11 (S.D.N.Y. May 22,

⁹ Defendant also does not raise the issue whether Plaintiff has statutory standing to bring his claim under Section 349. *See Fishon v. Peloton Interactive, Inc.*, 2020 WL 6564755, at *11–14 (S.D.N.Y. Nov. 9, 2020). “Unlike Article III standing, which ordinarily should be determined before reaching the merits, statutory standing may be assumed for the purposes of deciding whether the plaintiff otherwise has a viable cause of action.” *Coan v. Kaufman*, 457 F.3d 250, 256 (2d Cir. 2006) (internal citations omitted) (citing *Steel Co. v. Citizens for a Better Env.*, 523 U.S. 83, 94–95, 97 (1998)). Thus, because it is not raised, the Court does not address whether Plaintiff has statutory standing under New York law.

2013). Though “[o]rdinarily, the question of whether a business practice is deceptive is a question of fact not appropriately resolved on a motion to dismiss,” *Hertz Corp. v. Accenture LLP*, 2019 WL 5537997, at *4 (S.D.N.Y. Oct. 25, 2019), a court may make this determination as a matter of law, *Fink v. Time Warner Cable*, 714 F.3d 739, 741 (2d Cir. 2013).

Plaintiff claims Defendant engaged in the following deceptive acts and practices:

- (1) misrepresenting the safety and security of the assets entrusted to it;
- (2) failing to disclose to Mr. Yuille that Uphold’s platform was not secure and sufficient to safeguard his assets;
- (3) failing to properly monitor activity on its platform; and
- (4) deliberately or recklessly failing to safeguard and protect Mr. Yuille’s personal information and assets contained in Mr. Yuille’s account after enticing Mr. Yuille to place significant assets in his Uphold account through promotion of Uphold’s purportedly secure platforms.

Compl. ¶ 79. Defendant argues that Plaintiff’s claim must fail because “he has not, because he cannot, allege why or how any of the cited statements were false or misleading.” Dkt. No. 20 at 8. Plaintiff counters that he adequately makes out a Section 349 claim because he “alleges that Uphold advertised itself to consumers as a highly secure platform when it was not providing the security measures it promised, was not compliant with the security standards to which it purported to adhere, and did not even meet the basic requirements to operate legally in the state whose laws it assured consumers (via its terms of service) applied to the parties’ dealings.” Dkt. No. 23 at 11.

Plaintiff alleges that Uphold made affirmative “misrepresent[ations about] the safety and security of the assets entrusted to it.” Compl. ¶ 79. Plaintiff does not allege that any of the affirmative statements Uphold made were false or misleading when they were made. *See id.* ¶¶ 3–4, 19–20. On the Security page of its website, Uphold made both general statements about the security of its platform—including that “[s]ecurity is in our DNA,” “[o]ur number one priority is to protect you, your money, and your information” and “[s]ecurity is built into our systems and culture,” *id.* ¶¶ 3, 19—and specific statements about the security of its platform—

including that it “respond[s] immediately to any detected threat” and that its “providers undergo appropriate due diligence checks,” *id.* ¶ 20. The general statements made by Uphold, with the exception of the reference to security being Uphold’s “number one priority,” are not actionable under Section 349—they are puffery. Puffery “may occur in the form of ‘a general claim of superiority over comparable products,’ or, alternatively, as ‘an exaggerated, blustering, and boasting statement upon which no reasonable buyer would be justified in relying.’” *Weight Watchers Int’l, Inc. v. Noom, Inc.*, 403 F. Supp. 3d 361, 369-70 (S.D.N.Y. 2019) (quoting *Time Warner Cable*, 497 F.3d at 160). “Put another way, a plaintiff ‘must allege a statement specific enough to be falsifiable.’” *Doe v. Uber Techs., Inc.*, 551 F. Supp. 3d 341, 366 (S.D.N.Y. 2021) (citation omitted). Here, Uphold’s statements that “[s]ecurity is in our DNA” and that “[s]ecurity is built into our systems and culture” are prototypical examples of puffery; no reasonable consumer could have relied on those statements to understand either that Defendant had built specific security systems into its platform or that the Account would be immune to attacks by third-party hackers. *See id.* at 366–67 (“Statements that an Uber ride is ‘safe’ or that the ‘Uber experience has been designed from the group up with your safety in mind’ are general statements that ‘convey only the seller’s opinion that its product is superior, such that no consumer could claim to have justifiably relied on them.’” (quoting *Fusco v. Uber Techs., Inc.*, 2018 WL 3618232, at *6 (E.D. Pa. July 27, 2018))).

Uphold’s more specific statements are not puffery but they cannot support Plaintiff’s Section 349 claim because Plaintiff fails to allege that any of these statements were false when made.¹⁰ Although Plaintiff argues that the Complaint “sufficiently alleges that Uphold failed to

¹⁰ The statement that security is Uphold’s “number one priority” is arguably puffery. The Court, however, need not reach a conclusion on that issue because even if it could be read as a statement of fact, Plaintiff has not pleaded that it was false or misleading.

abide by the aforementioned representations,” Dkt. No. 23 at 9, he does not point to any alleged facts in his Complaint or otherwise, and the Court cannot discern any such facts, that suggest that the specific representations made by Uphold were in fact false. For example, there is no allegation that despite Uphold’s representation that it deployed “layered defenses to limit the scope and depth of potential attacks, as well as sophisticated encryption,” Compl. ¶ 20, Uphold did not employ layered defenses or sophisticated encryption, or that despite the representation that Uphold “monitors systems year-round and responds immediately to any detected threat,” *id.*, that it did not monitor its systems or detect a threat with respect to Yuille’s account or the accounts of others such that Uphold’s representation that it would “respond[] immediately” might be considered false. In fact, Plaintiff does not appear to dispute that all of the statements detailed in the Complaint were true when made. *See* Dkt. No. 23 at 8 (“[T]here is no requirement that a plaintiff allege that a statement was false or how it was false” under Section 349.).

Instead, Plaintiff suggests that, even if the statements were true, Defendant’s statements created the *impression* that Uphold was a secure cryptocurrency platform when in fact it was not, in violation of Section 349. *See* Compl. ¶ 3 (“Uphold . . . holds itself out as being one of the most secure cryptocurrency platforms and touts as such on its website.”); *see also id.* ¶¶ 19, 77. In the analogous context of the antifraud provisions of the Federal Trade Commission Act, 15 U.S.C. § 45 (“FTCA”),¹¹ courts have recognized that a statement that is literally true in its component parts may still be misleading when read in its entirety. *See F. T. C. v. Sterling Drug, Inc.*, 317 F.2d 669, 675 (2d Cir. 1963) (“Advertisements as a whole may be completely

¹¹ New York’s Consumer Protection Act, which was codified in part through Section 349, was crafted based on the FTCA and is considered to be the state “counterpart” to the FTCA. *See Oswego*, 647 N.E.2d at 745; *see also Goshen*, 774 N.E.2d at 1194–95.

misleading although every sentence separately considered is literally true. This may be because things are omitted that should be said, or because advertisements are composed or purposefully printed in such way as to mislead.” (quoting *Donaldson v. Read Magazine*, 333 U.S. 178, 188 (1948))). A statement that is literally true can be misleading in context where (1) “the statement is removed from its context and the nondisclosure of its context renders the statement misleading” or (2) “the statement in context has two or more commonly understood meanings, one of which is deceptive.” *Id.* at 674–75; see also *F.T.C. v. Med. Billers Network, Inc.*, 543 F. Supp. 2d 283, 304 (S.D.N.Y. 2008) (collecting cases) (“A court should focus on the overall impression created by the advertising, not its ‘literal truth or falsity.’”). Thus, for example, “[t]he failure to disclose material information may cause an advertisement to be false or deceptive even though it does not state false facts.” *Med. Billers Network, Inc.*, 543 F. Supp. 2d at 304 (quoting *Katharine Gibbs School (Inc.) v. FTC*, 612 F.2d 658, 665 (2d Cir. 1979)); cf. *Himmelstein, McConnell, Gribben, Donoghue & Joseph, LLP v. Matthew Bender & Co., Inc.*, 171 N.E.3d 1192, 1199 (N.Y. 2021) (suggesting that it is “the overall impression of the representations [being] misleading” that matters for Section 349 purposes).

Plaintiff’s argument that Defendant created the false *impression* that its cryptocurrency platform was safe suffers from two related flaws. First, a reasonable consumer could not have interpreted the statements in the Complaint in this way.¹² A reasonable consumer could understand the statements alleged in the Complaint to suggest that Uphold deployed specific security protocols that it believed to be reasonably adequate, but the statements cannot be read to

¹² How Plaintiff himself interpreted the statements is irrelevant to the analysis under Section 349. See *Rivera v. Navient Sols., LLC*, 2020 WL 4895698, at *10 (S.D.N.Y. Aug. 19, 2020) (The question under Section 349 is whether the act or practice “would have been confusing or misleading to a reasonable consumer, and not to the plaintiff before the Court based on his or her own idiosyncratic facts.”)

provide an assurance that there would be no circumstances under which Uphold’s security systems would fail or that its accounts would be invulnerable to third-party attacks. *Cf. Uber Technologies*, 551 F. Supp. 3d at 368 (noting that “language that Uber is ‘committed’ to connecting consumers to the ‘safest ride on the road’ is aspirational puffery. . . . No reasonable consumer could understand the statement to warrant that Uber has been successful in its commitment and that by accepting a ride in an Uber car, the consumer will in fact receive the safest ride on the road.”). Second, even assuming that Defendant’s statements created an impression that Uphold had one of the most secure cybersecurity platforms, the allegations made by Plaintiff—that a single account (Plaintiff’s own) was compromised and that Defendant failed to respond sufficiently timely to an outside attack—do not demonstrate that the impression was false when Uphold communicated that impression to consumers. Plaintiff has not pled that Uphold was not one of the most, if not the most, secure cryptocurrency platform at the time the statements were made and the fact that a single account was hacked does not undermine that conclusion.

For this reason, the Court finds the case that Defendant principally relies on, *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 49 Misc. 3d 1027 (N.Y. Sup. Ct. 2015), persuasive. In *Abdale*, the plaintiffs alleged that “the defendants ‘maintained a privacy policy guaranteeing that plaintiffs’ protected health information would not be released to any unauthorized third parties without plaintiffs’ consent.’” *Id.* at 1038–39. The court held that the plaintiffs failed to state a Section 349 claim because “the statements allegedly made by defendants in the privacy policy and online notices do not constitute an unlimited guaranty that patient information could not be stolen or that computerized data could not be hacked.” *Id.* at 1039. Similarly, here, the statements that Uphold made could not have communicated the impression that Uphold’s

platform was so secure that no hackers, no matter how talented, could penetrate Uphold's platform and that assets stored in Uphold's account were safe from all potential harms.

Plaintiff principally relies on an out-of-district case, *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2017), *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018), to support his argument that he has adequately pled a Section 349 claim. *Fero*, however, is distinguishable. In *Fero*, the plaintiffs alleged that the defendants "misrepresented and advertised that they 'would maintain adequate data privacy and security practices and procedures to safeguard New York Class Members' [personally identifiable information] and [protected health information] from unauthorized disclosure, release, data breaches, and cyber attack.'" *Id.* at 774. The plaintiffs further alleged that the defendants "had reason to know that their data security was inadequate both before the data breach started and after it was discovered by [the d]efendants." *Id.* at 744. The court thus concluded that the defendants' "representations in their privacy policies and on their websites concerning data security . . . would lead a reasonable consumer to believe that the Excellus Defendants were providing more adequate data security than they purportedly were." *Id.* at 776. Plaintiff here does not allege that Defendant made blanket representations about the *adequacy* of its security and that Defendant knew its security was inadequate. Rather, Plaintiff alleges that Defendant made representations about its security being "robust" and "state of the art" and about the types of security procedures that it deployed—and unlike in *Fero*, Plaintiff does not specify how any of those statements were false. *See* Compl. ¶¶ 3, 20.

Plaintiff also alleges that Defendant violated Section 349 because it failed to disclose that its "platform was not secure and sufficient to safeguard his assets." *Id.* ¶ 79. The New York Court of Appeals has held that a Section 349 claim can also be founded on a materially deceptive

omission. *See Fishon*, 620 F. Supp. 3d at 104–05 (S.D.N.Y. 2022) (discussing, *inter alia*, *Oswego*, 647 N.E.2d 741). An omission is actionable under Section 349, “as the weight of authority now understands the law, where a defendant fails to supply a consumer information that it alone possesses, and where that information would be material or important to a reasonable consumer and where the consumer could not have reasonably obtained the information other than through the defendant.” *Id.* at 104. Thus, “[t]he key” to a Section 349 omission claim “is that the defendant ‘possess’ the information that the plaintiff claims it improperly withheld.” *In re Sling Media Slingbox Advert. Litig.*, 202 F. Supp. 3d 352, 359 (S.D.N.Y. 2016); *see also id.* (to state a claim, the plaintiff must “plausibly allege[] that the . . . [d]efendants had knowledge of the [material information] and failed to disclose or actively concealed such information.” (alterations in original) (quoting *Woods v. Maytag Co.*, 807 F. Supp. 2d 112, 129 (E.D.N.Y.2011))). But “the statute surely does not require businesses to ascertain consumers’ individual needs and guarantee that each consumer has all relevant information specific to its situation.” *Oswego*, 647 N.E.2d at 745.

Plaintiff’s Section 349 claim cannot be saved by reframing it as one for an omission. Plaintiff does not allege any material information in Defendant’s possession that it failed to disclose to its consumers. Plaintiff does not, for example, allege that Defendant’s security procedures were inadequate to deal with common threats or that Defendant knew there would be . . . Further, the Complaint does not adequately allege that Uphold *knew* that its platform was not secure or sufficient to safeguard certain assets.¹³ *See In re Sling Media Slingbox Advert. Litig.*,

¹³ Plaintiff does allege that at some unknown time Uphold “recognized a massive increase in activity by ‘scammers and bad actors’” and noted that its “fraud and compliance policies and systems ‘are constantly contending with the advancements of scammers and bad actors, but were not optimized to cope with the 50x increase in volumes we’ve seen.’” Compl. ¶ 29 (citation omitted). Based in part on this statement, Plaintiff alleges that “Uphold knew of the risks that its

202 F. Supp. 3d at 359–60 (dismissing omission-based Section 349 claim because Plaintiff “failed to plead facts sufficient to lead to the reasonable inference” that the defendant “had knowledge of the information Plaintiffs allege it failed to disclose at the time Plaintiffs made their purchases”).

Finally, Plaintiff alleges that Defendant violated Section 349 by “failing to properly monitor activity on its platform; and . . . deliberately or recklessly failing to safeguard and protect Mr. Yuille’s personal information and assets contained in Mr. Yuille’s account.” Compl. ¶ 79. But that conduct, even if assumed to be true, cannot give rise to a claim under Section 349.

customers’ accounts could be compromised or hacked . . . [y]et it failed to take appropriate action to safeguard customers’ data and information from being accessed by unauthorized third parties.” *Id.* ¶ 32. However, in context, Defendant’s statement about the risk of hacking cannot rescue Plaintiff’s omission claim because the only facts that Plaintiff pleads related to its omissions claim come from Defendant’s statement *disclosing* to its customers that its security features were not optimized to deal with the increase in activity from scammers and other bad actors. The statement does not support that Uphold had knowledge about the weaknesses of its security practices that it omitted to disclose nor does Plaintiff allege that at some earlier point in time, Defendant recognized that its security features were inadequate and then failed to disclose that knowledge to its customers before the article was published, causing Plaintiff a cognizable injury under Section 349.

It also is unclear, even accepting Plaintiff’s allegations as true, whether the statement indicates that there were security flaws in Uphold’s platform. Uphold’s statement was made in an article on Uphold’s website titled “Improving customer support.” *See id.* ¶ 28 n.16. In that article, Uphold apologized for the “temporary account restrictions and slow response times” resulting from the increase in “scammers and bad actors” and took certain actions, including decreasing the number of situation in which it would restrict a customer’s account and allowing customers to change certain settings and pieces of information without contacting customer support. *Id.* ¶¶ 28–30 (citations omitted). One plausible inference is that Uphold believed its security practices were overinclusive and that it was restricting accounts more frequently than required to guard the security of accounts on its Platform. Whether or not that conclusion was correct can reasonably be debated, but the lack of “optimiz[ation]” of security features that Uphold acknowledged was not a reference to the security features being inadequate to protect an account but reflected a belief, at least as conveyed through the article, that its security settings were too stringent and thus more protective than necessary. Moreover, as noted above, even assuming that Uphold’s article can be interpreted as an acknowledgement that it had knowledge that its security procedures were inadequate, the article does not establish that Uphold withheld that information because the article *discloses* that fact to Uphold’s consumers.

Section 349 applies to both “acts” and “practices,” but such acts and practices must be “[d]eceptive.” NYGBL § 349. Thus, a plaintiff must at least plausibly allege that the defendant knew it was omitting to act and that its omission would be misleading to a reasonable consumer. “New York’s Consumer Protection Act—[which contains Section 349]—was enacted to provide consumers with a means of redress for injuries caused by unlawfully deceptive acts and practices.” *Goshen*, 774 N.E.2d at 1194. Though the legislation is “intentionally broad, applying to virtually all economic activity,” *id.* (internal quotation marks and citation omitted), its purpose is limited “to secur[ing] an ‘honest market place’ where ‘trust,’ and not deception, prevails,” *id.* (citation omitted). Thus, mere negligence or recklessness cannot give rise to a claim under Section 349; a marketplace is no less honest and the marketplace no less based on trust if a business fails to act but has no knowledge that it is failing to act or if the failure to act is not misleading to a reasonable consumer. Assuming, what is not challenged here, that Plaintiff has plausibly alleged that Defendant did not properly monitor activity on its platform and that it failed to safeguard Plaintiff’s account, Plaintiff has not plausibly alleged that Defendant *knew* that it was failing to adequately monitor its platform and to protect accounts on the platform and that not disclosing that fact was somehow misleading. Plaintiff specifically pleads that Defendant’s failure to safeguard Yuille’s account could have been “reckless[]” and he does not allege that Defendant knew it was improperly monitoring account activity. Compl. ¶ 79. Section 349 does not create a free-floating obligation on all custodians of assets to safeguard those assets. The law guards against deception. Protection against the theft of assets, and the corresponding requirement of a bailee to monitor activity on a platform must be found, if at all, in other bodies of law. *See Nick’s Garage, Inc. v. Progressive Cas. Ins. Co.*, 875 F.3d 107, 127 (2d Cir. 2017)

("[A]cts cannot be re-characterized as 'deceptive' simply on the grounds that they violate another statute."). Accordingly, Plaintiff's Section 349 claim fails as a matter of law.

III. Count IV: Intentional Misrepresentation

Uphold argues that Plaintiff's intentional misrepresentation claim must fail because he "has not sufficiently pled that any of Uphold's statements were false, nor has Plaintiff made any attempt to establish that Uphold intended to defraud its customers through those purported representations." Dkt. No. 20 at 9–10. Plaintiff counters that it has pled sufficient facts to establish that Uphold made misrepresentations of presently existing facts with the requisite intent to defraud. Dkt. No. 23 at 11–12. The Court finds that Plaintiff has not stated a claim for intentional misrepresentation.

To state a claim for intentional misrepresentation under New York law, a plaintiff must plead the elements of fraud, *see Assoun v. Assoun*, 2015 WL 110106, at *5 (S.D.N.Y. Jan. 7, 2015) ("[A] claim for intentional misrepresentation, . . . under New York law, is identical to a claim for fraud."): "(1) a material misrepresentation or omission of a fact, (2) knowledge of that fact's falsity, (3) an intent to induce reliance, (4) justifiable reliance by the plaintiff, and (5) damages." *Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC*, 797 F.3d 160, 170 (2d Cir. 2015) (citing *Eurycleia Partners, LP v. Seward & Kissel, LLP*, 910 N.E.2d 976 (N.Y. 2009)). Fraud-based claims must satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b), which require that fraud be pled "with particularity." Fed. R. Civ. P. 9(b). To comply with Rule 9(b)'s heightened pleading requirements, "the complaint must: (1) specify the statements that the plaintiff contends were fraudulent, (2) identify the speaker, (3) state where and when the statements were made, and (4) explain why the statements were fraudulent." *Lerner v. Fleet Bank, N.A.*, 459 F.3d 273, 290 (2d Cir. 2006) (internal quotation marks and citation omitted). "Although Rule 9(b) contains a heightened [pleading] standard, it

also relaxes the standard for pleading fraudulent intent: ‘Malice, intent, knowledge, and other conditions of a person’s mind may be alleged generally.’” *Duran v. Henkel of Am., Inc.*, 450 F. Supp. 3d 337, 353 (S.D.N.Y. 2020) (quoting Fed. R. Civ. P. 9(b)). This relaxed standard, however, is not “license to base claims of fraud on speculation and conclusory allegations [P]laintiffs must allege facts that give rise to a strong inference of fraudulent intent.” *Lerner*, 459 F.3d at 290 (quoting *Acito v. IMCERA Group, Inc.*, 47 F.3d 47, 52 (2d Cir. 1995)). Plaintiffs can establish this “strong inference” either “(a) by alleging facts to show that defendants had both motive and opportunity to commit fraud, or (b) by alleging facts that constitute strong circumstantial evidence of conscious misbehavior or recklessness.” *Id.* (quoting *Shields v. Citytrust Bancorp, Inc.*, 25 F.3d 1124, 1128 (2d Cir. 1994)) (internal quotation marks omitted). *See generally Green Star Energy Sols., LLC v. Edison Properties, LLC*, 2022 WL 16540835, at *7 (S.D.N.Y. Oct. 28, 2022).

Plaintiff’s claim fails for at least two reasons. First, Plaintiff has not pleaded facts that would establish that Uphold *knew* that any statements it made were false, or acted with reckless disregard to its truth. Plaintiff alleges that “Uphold knew of the risks that its customers’ accounts could be compromised or hacked.” Compl. ¶ 32. However, the facts upon which that allegation is based—that Uphold “recognized a massive increase in activity by ‘scammers and bad actors’” and noted that its “fraud and compliance policies and systems ‘are constantly contending with the advancements of scammers and bad actors, but were not optimized to cope with the 50x increase in volumes we’ve seen,’” *id.* ¶ 29 (citation omitted)—do not give rise to a “strong inference of fraudulent intent.” *Lerner*, 459 F.3d at 290 (citation omitted). Rather, they suggest that at some later point in time, Defendant recognized certain vulnerabilities in its security procedures, disclosed those vulnerabilities to its customers, and sought to correct them.

See U.S. ex rel. O'Donnell v. Countrywide Home Loans, Inc., 822 F.3d 650, 658 (2d Cir. 2016) (“It is emphatically the case—and has been for more than a century—that a representation is fraudulent only if made with the contemporaneous intent to defraud—*i.e.*, the statement was knowingly or recklessly false and made with the intent to induce harmful reliance.”); *see also Ultramares Corp. v. Touche*, 174 N.E. 441, 447 (N.Y. 1931) (Cardozo, C.J.) (noting that “[a] representation” must be “knowingly false”).

Second, Plaintiff has not met the heightened pleadings standard of Rule 9(b). Plaintiff argues that he has met this standard because he has pleaded “Yuille expressly pleads the times when he reviewed Uphold’s deceptive and misleading advertising.” Dkt. No. 23 at 13. But Yuille never pleads that he reviewed the statements listed in the Complaint or that the statements listed in the Complaint were available when he registered for the Account. The Security page that Yuille cites was “last visited [on] April 18, 2022,” *see, e.g.*, Compl. ¶ 4 n.2, months after Yuille opened the Account and the Account was hacked, *see id.* ¶¶ 21, 46–54, and there are no allegations that the same representations were available when Yuille signed up for the account. Thus, Plaintiff has failed to allege when the allegedly fraudulent statements were made. *See Exact Invs. LLC v. Vesnaverboth*, 2022 WL 17782087, at *4 (E.D.N.Y. July 18, 2022) (dismissing a fraud claim because, *inter alia*, the plaintiff did not allege “when the statement was made,” and thus failed to satisfy Rule 9(b)); *Sendar Co. v. Megaware Inc.*, 705 F. Supp. 159, 161 (S.D.N.Y. 1989) (holding that allegations of complaint failed to meet heightened standard of Rule 9(b) because “[t]he allegations fail to specify the date on which fraudulent statements were made, merely alleging that statements were made some time during a two month period”).

Nor does the Complaint explain how the statements were fraudulent with any particularity. The Complaint alleges that Uphold made misrepresentations when it “held itself

out as being one of the most secure cryptocurrency platforms and touts as such on its website.” Compl. ¶ 88. It further alleges that Uphold made misrepresentations when it represented that (1) it used layered defenses and sophisticated encryption; (3) conducted “security audits and penetration testing” of its platform; (4) monitored its system and “responds immediately to any detected threat”; and (5) does email verification if it detected anything “untoward.” *Id.* ¶ 89. However, although the Complaint refers to these statements as “misrepresentations,” *see, e.g., id.* ¶¶ 88–92, and states that they were “false,” *id.* ¶ 55, there are no allegations that suggest why they were false or fraudulent. Plaintiff, for example, does not allege that Uphold was not one of the most secure cryptocurrency platforms or that it did not use layered defenses and sophisticated encryption or monitored and tested its systems or performed email verification. *See Rombach v. Chang*, 355 F.3d 164, 175 (2d Cir. 2004) (“To meet the pleading requirement of Rule 9(b), plaintiffs cannot rest on their say-so that these statements are fraudulent; they must explain why.”); *Gross v. Diversified Mortg. Invs.*, 438 F. Supp. 190, 195 (S.D.N.Y. 1977) (“To satisfy Rule 9(b) plaintiffs must specify in what respects each of the statements were false and misleading.”). Notably, the reasonable inferences that can be drawn from Plaintiff’s allegation that his account was hacked and his cryptocurrency was stolen does not support the fact that any of these statements were fraudulent: It does not establish, for example, that Uphold detected anything “untoward” that would have facilitated email verification (or that Uphold failed to perform the requisite email verification after his email address was changed by the hackers) or that Uphold detected any threats that an immediate response was necessary. Plaintiff’s allegations thus fail to satisfy the heightened pleading standards of Rule 9(b).

Because Plaintiff has failed to plead that Defendant knew its statements were false when they were made and has failed to meet the heightened pleadings standards of Rule 9(b), it does not address the other bases on which Plaintiff’s claim might also fail.

IV. Count VI: Gross Negligence

Uphold argues that Plaintiff’s gross negligence claim fails as a matter of law because Plaintiff has not alleged that Uphold’s conduct was reckless or intentional, which is necessary to establish that Uphold was grossly negligent. Dkt. No. 20 at 12. Plaintiff counters that Defendant’s conduct in failing to safeguard Plaintiff’s account constitutes gross negligence under New York law. Dkt. No. 23 at 14–15. Uphold’s argument is without merit.

Under New York law, “[t]o prevail on a claim for gross negligence, plaintiff must establish” the elements necessary to prevail on a claim for negligence—(1) duty; (2) breach; and (3) injury—plus a fourth element, namely, that defendant’s conduct “evinces a reckless disregard for the rights of others or ‘smacks’ of intentional wrongdoing.” *Farash v. Cont’l Airlines, Inc.*, 574 F. Supp. 2d 356, 367–68 (S.D.N.Y. 2008), *aff’d*, 337 F. App’x 7 (2d Cir. 2009) (Sullivan, J.) (quoting *AT&T v. City of New York*, 83 F.3d 549, 556 (2d Cir. 1996)). Uphold does not dispute that it had a duty to Plaintiff, it breached that duty, and that its breach caused Plaintiff an injury. It argues instead that, because the loss was caused by the act of a third-party criminal, its conduct could not have been reckless or intentional.¹⁴

¹⁴ Uphold does argue that “[b]ecause Plaintiff does not plead that Uphold owed him a duty of care to protect against the conduct of third-party criminals . . . , his gross negligence claim fails along with his negligence claim” and that Plaintiff cannot “establish a claim for negligence.” Dkt. No. 20 at 12. It is unclear whether Defendant is arguing (1) that it owed no duty to Plaintiff from which a claim for negligence or gross negligence could lie; or (2) whether any duty it owes would not be violated by the failure to protect against the conduct of third-party criminals, *i.e.*, that the failure to protect against criminals could not be reckless. Defendant’s arguments and the cases it cites focuses on whether a duty could have been violated by third-party criminals and it is that formulation of Defendant’s argument that the Court addresses.

“To constitute gross negligence, the act or omission must be of an aggravated character, as distinguished from the failure to exercise ordinary care.” *Am. Auto. Ins. Co. v. Rest Assured Alarm Sys., Inc.*, 786 F. Supp. 2d 798, 807 (S.D.N.Y. 2011) (citation omitted). New York courts have analyzed whether conduct is sufficiently aggravated to constitute gross negligence in an analogous context: the provision and maintenance of fire and burglar alarm services. “Generally, no issue of gross negligence is raised where the claim is based upon either inappropriate installation of an alarm system or an inappropriate response to an alarm. . . . On the other hand, a sufficient issue regarding gross negligence has been held to have been raised in cases referred to as including ‘outrageous acts of folly.’” *Metro. Prop. & Cas. Ins. Co. v. Budd Morgan Cent. Station Alarm Co.*, 95 F. Supp. 2d 118, 122–23 (E.D.N.Y. 2000) (citation omitted). Thus, for example, the New York Court of Appeals has found that a plaintiff “alleged much more than mere failure to install a proper working alarm system and inspect it,” because the plaintiff alleged that “defendants had knowledge—for weeks, if not months—that the equipment had been malfunctioning” and “that defendants not only failed to investigate the source of their equipment malfunction, but they failed to put anyone at the branch on notice of the potential security breach.” *Abacus Fed. Sav. Bank v. ADT Sec. Servs., Inc.*, 967 N.E.2d 666, 669 (N.Y. 2012). Similarly, the First Department has found that a jury could find that an alarm company was grossly negligent when it failed to send guards to a jewelry manufacturer eleven hours after a weekend break-in and the manufacturer had not alerted the alarm company that it would be open over the weekend. *Rand & Paseka Mfg. Co. v. Holmes Prot. Inc.*, 515 N.Y.S.2d 468, 469–70 (1st Dep’t 1987); *see also Hanover Ins. Co. v. D & W Cent. Station Alarm Co.*, 560 N.Y.S.2d 293, 295–96 (1st Dep’t 1990) (finding summary judgment for alarm company inappropriate where the record indicated that the alarm company received three signals over four hours, did not

notify the police, and directed the guard sent to investigate the issue to “forget the assignment” when he encountered difficulty entering the building). But courts have found insufficient to find gross negligence “failure to wire a skylight,” which burglars broke through to steal paintings, *Colnaghi, U.S.A., Ltd. v. Jewelers Prot. Servs., Ltd.*, 611 N.E.2d 282, 284 (N.Y. 1993), or “an alarm company’s delayed or inadequate response to an alarm signal, without more,” *Abacus Fed. Sav. Bank v. ADT Sec. Servs., Inc.*, 908 N.Y.S.2d 654, 656 (1st Dep’t 2010), *aff’d as modified*, 967 N.E.2d 666 (collecting cases).

Based on these standards, Plaintiff has alleged sufficient facts to plead that Defendant’s conduct was grossly negligent. Here, as in the alarm system context, Plaintiff alleges that Uphold was responsible for monitoring and maintaining the security of the accounts on its platform. *See* Compl. ¶¶ 19–21. The Complaint alleges that Uphold was aware that there was “a massive increase in activity by ‘scammers and bad actors.’” *Id.* ¶ 29. Further, the Complaint alleges that the hackers “triggered the alarm” on Plaintiff’s account several times before successfully gaining control of his account: Between December 7 and December 9, a third party tried and failed to change the Account’s password five times and on December 7, a third party unsuccessfully attempted to log into Plaintiff’s account from Nigeria. *Id.* ¶¶ 46–47. Finally, on December 9 at 10:48 a.m., the third party changed the Account’s password and eight minutes later, changed the e-mail address associated with the Account. *Id.* ¶ 48. And once the third party was able to gain control of the Account, Plaintiff warned Uphold that he was unable to access the Account, writing “HELP, I am locked out of my account. I enter the username and password I have been using for past several months, and I get a message that they do not match your records. . . . Please communicate with me.” *Id.* ¶ 51. Defendant responded by telling Plaintiff to check his spam folder for the password-reset verification emails. *Id.* ¶ 52. Then, approximately

eight hours after Plaintiff's email explicitly alerting Defendant to the breach of the Account, the third party began transferring Bitcoin from the Account, activity which continued until 5:00 p.m. on December 11, 2021, at which point approximately \$5,000,000 worth of Bitcoin was stolen.

Id. ¶ 54. The conduct alleged in the Complaint is more than a mere failure to adequately secure or monitor the platform; rather, Plaintiff alleges that Uphold knew that there was a rise in hacking activity, was explicitly told about the potential security breach to the Account, and failed to act for approximately two-and-one-half days while a third party transferred \$5,000,000 worth of Bitcoin from the Account.

Accordingly, Plaintiff's allegation of gross negligence is plausible and Defendant's motion to dismiss the gross negligence claim for failure to allege reckless or intentional conduct is denied.

V. Count VII: Declaratory Judgment

Finally, Defendant moves to dismiss Count VII, which seeks a declaratory judgment under 28 U.S.C. § 2201 that Section 12.4 of the Terms and Conditions unenforceable. Section 12.4 limits Uphold's "aggregate liability . . . to the greater of (a) the actual fees paid to us by you in the preceding three (3) months or (b) US\$100 dollars" and disclaims liability for "any lost profits or other consequential, special, indirect, or incidental damages arising out of or in connection with these terms and conditions or the Platform." Dkt. No. 19.2 § 12.4. Plaintiff claims that the provision "is unconscionable, void as against public policy, attempts to disclaim statutory and other legal duties for which it cannot contractually avoid, and violates 15 U.S.C. § 1693*l*, which provides that a consumer may not waive by agreement any right conferred, or cause of action created, by the EFTA." Compl. ¶ 118. Defendant argues that the Complaint does not establish procedural or substantive unconscionability and the EFTA argument fails because the EFTA does not apply to the Account. Dkt. No. 20 at 13–14. Plaintiff counters that

the provision is substantively unconscionable and is void under New York and federal law because it precludes Plaintiff from pursuing his statutory rights.¹⁵ Dkt. No. 23 at 16–17.

Under New York law, contractual limitation of liability clauses are generally enforceable against the non-breaching party. *See Camofi Master LDC v. Coll. P'ship, Inc.*, 452 F. Supp. 2d 462, 478 (S.D.N.Y. 2006) (Chin, J.) (“The New York State Court of Appeals recognizes that courts should normally honor liability limiting provisions.” (citing *Met. Life Ins. Co. v. Noble Lowndes Int’l, Inc.*, 643 N.E.2d 504, 507 (N.Y. 1994))). However, a Court will not enforce a limitation of liability provision if “the provision is ‘the result of unconscionable conduct or unequal bargaining power between the parties.’” *Id.* (quoting *DynCorp v. GTE Corp.*, 215 F. Supp. 2d 308, 317 (S.D.N.Y. 2002)); *see also Biotronik A.G. v. Conor Medsystems Ireland, Ltd.*, 11 N.E.3d 676, 692 (N.Y. 2014) (Read, J. dissenting) (“[I]f contracting parties agree to a limitation-of-liability provision, it will be enforced unless unconscionable, even if it leaves a non-breaching party without a remedy.”).

“Under New York law, a contract is unconscionable when it ‘is so grossly unreasonable or unconscionable in the light of the mores and business practices of the time and place as to be unenforceable [sic] according to its literal terms.’” *Nayal v. HIP Network Servs. IPA, Inc.*, 620 F. Supp. 2d 566, 571 (S.D.N.Y. 2009) (quoting *Gillman v. Chase Manhattan Bank, N.A.*, 534 N.E.2d 824, 828 (N.Y. 1988)). “Generally, there must be a showing that such a contract is both procedurally and substantively unconscionable.” *Id.* “The procedural element of unconscionability concerns the contract formation process and the alleged lack of meaningful

¹⁵ Because Plaintiff’s EFTA and NYGBL claims fail, *see supra* Sections I and II, and because the Court does not at this time address whether Plaintiff has a viable claim under the MCPA, *see infra* note 18, the Court does not at this point address Plaintiff’s claim that Section 12.4 of the Terms and Conditions is void insofar as it precludes Plaintiff from pursuing certain statutory rights.

choice; the substantive element looks to the content of the contract, per se.” *Id.* (quoting *State v. Wolowitz*, 468 N.Y.S.2d 131, 145 (2d Dep’t 1983)); *see also Desiderio v. Nat’l Ass’n of Sec. Dealers, Inc.*, 191 F.3d 198, 207 (2d Cir. 1999) (“A contract or clause is unconscionable when there is an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party.” (internal quotation marks and citation omitted)). “Procedural and substantive unconscionability are weighed on a ‘sliding scale’—the more questionable the meaningfulness of choice, the less imbalance in a contract’s terms should be tolerated and vice versa.” *Mayaguez S.A. v. Citigroup, Inc.*, 2018 WL 1587597, at *12 (S.D.N.Y. Mar. 28, 2018) (quoting *David v. #1 Mktg. Serv., Inc.*, 979 N.Y.S.2d 375, 378–79 (2d Dep’t 2014)). The Complaint does not contain well-pled allegations of either procedural or substantive unconscionability.

Plaintiff does not argue that the clause is procedurally unconscionable. *See* Dkt. No. 23 at 16 (only arguing that “Yuille has clearly pled that the Exculpation Clause is substantively unconscionable”). “The procedural element of unconscionability requires an examination of the contract formation process and the alleged lack of meaningful choice.” *Gillman*, 534 N.E.2d at 828. “The focus is on such matters as the size and commercial setting of the transaction, whether deceptive or high-pressured tactics were employed, the use of fine print in the contract, the experience and education of the party claiming unconscionability, and whether there was disparity in bargaining power.” *Id.* (internal citation omitted). The Complaint contains no allegations related to the formation of the Terms and Conditions. The Complaint alleges that Yuille began looking for a cryptocurrency exchange to hold his Bitcoin in July 2021, that he selected Uphold to be that cryptocurrency exchange, and that he transferred his Bitcoin to the Account in August 2021. Compl. ¶¶ 21, 24. It does not allege when the contract was formed,

how it was formed, and under what circumstances it was formed. Thus, Plaintiff's allegations do not establish that Section 12.4 of the Terms and Conditions is procedurally unconscionable. See *Passelaigue v. Getty Images (US), Inc.*, 2018 WL 1156011, at *5 (S.D.N.Y. Mar. 1, 2018) (concluding that agreement was not procedurally unconscionable because “[t]here are no allegations that [one of the defendants] did anything so as to effectively deprive Plaintiff of a meaningful choice”); *Don King Prods., Inc. v. Douglas*, 742 F. Supp. 778, 780 (S.D.N.Y. 1990) (finding no procedural unconscionability where there was “no allegation here that deceptive or high-pressure tactics were employed in concluding the contracts, that contract terms were concealed in fine print, or that there was a gross asymmetry in the experience and education of the parties, each of whom was represented by counsel throughout the course of their arms-length negotiations”).

Plaintiff relies primarily on substantive unconscionability. Substantive unconscionability looks at “the substance of the bargain to determine whether the terms were unreasonably favorable to the party against whom unconscionability is urged.” *KLS Diversified Master Fund, L.P. v. McDevitt*, 532 F. Supp. 3d 126, 137 (S.D.N.Y. 2021), *aff'd*, 2022 WL 2759055 (2d Cir. July 13, 2022) (quoting *Gillman*, 534 N.E.2d at 829). “While determinations of unconscionability are ordinarily based on [a] conclusion that both the procedural and substantive components are present, there have been exceptional cases where a provision of the contract is so outrageous as to warrant holding it unenforceable on the ground of substantive unconscionability alone.” *Ragone v. Atl. Video at Manhattan Ctr.*, 595 F.3d 115, 122 (2d Cir. 2010) (quoting *Gillman*, 534 N.E.2d at 829). Plaintiff has not pled that such a situation exists.

Plaintiff argues that Section 12.4 is substantively unconscionable because Yuille's losses amount not “50,000 times that amount to which Uphold seeks to limit its liability.” Dkt. No 23

at 16. However, this fact alone is insufficient to establish that the limitation on liability is so outrageous that the Court must find the provision unenforceable based on substantive unconscionability alone. As noted, there is nothing inherently suspect about a limitation of liability clause; New York courts consistently uphold them when they do not otherwise violate public policy. *See Optima Media Grp. Ltd. v. Bloomberg L.P.*, 2018 WL 1587074, at *7 (S.D.N.Y. Mar. 28, 2018) (Nathan, J.) (“Parties to a contract are generally free to allocate risks and limit liability as they choose. [They] may later regret their assumption of the risks of non-performance in this manner, but the courts let them lie on the bed they made.” (internal quotation marks and citations omitted)). Additionally, Plaintiff was not contractually obligated to take any actions as a result of the Terms and Conditions, including his decision to transfer \$5 million of Bitcoin into the Account, which he presumably made after the Terms and Conditions were entered into. Instead, he could have made a determination of how much Bitcoin to transfer to Uphold’s platform based on how risk was allocated by the limitation of liability clause. Thus, the fact that Plaintiff chose to transfer such a large amount of Bitcoin into the Account, and the ratio between Plaintiff’s loss and the maximum liability Uphold is contractually required to bear is so high, cannot alone serve as the basis for a finding that the provision was *ex ante* unconscionable. *See Spinelli v. Nat’l Football League*, 903 F.3d 185, 208 (2d Cir. 2018) (noting that, to be found unconscionable under New York law, a contractual provision must be “both procedurally and substantively unconscionable *when made*” (citation omitted)). Nor has Plaintiff made a showing that the provision is “so grossly unreasonable or unconscionable in light of the mores and business practices of the time and place.” *KLS Diversified Master Fund, L.P.*, 532 F. Supp. 3d at 137 (quoting *Red Fort Cap., Inc. v. Guardhouse Prods. LLC*, 2020 WL 5819549, at *9 (S.D.N.Y. Sept. 30, 2020)). Plaintiff has pled no facts suggesting the mores and business

practices of cryptocurrency platforms at the time he opened the Account. Accordingly, Count VII must be dismissed.¹⁶

CONCLUSION

The motion to dismiss is GRANTED IN PART and DENIED IN PART. The motion is GRANTED with respect to Counts I, II, IV, and VII.¹⁷ However, the motion is DENIED as to Counts III¹⁸ and VI. Plaintiff must file any amended complaint within thirty days of the date of this Opinion and Order.

¹⁶ The Court notes that to the degree that Plaintiff is able to prove gross negligence and to establish that Section 12.4 of the Terms and Conditions limits Plaintiff's recovery to nominal damages, the limitation-of-liability clause may be unenforceable under New York law. As a matter of public policy, New York courts will not enforce exculpatory or nominal damages clauses that limit liability for breaches of contract when the breach arises from grossly negligent conduct. *See Matter of Part 60 Put-Back Litig.*, 165 N.E.3d 180, 185–86 (N.Y. 2020) (“In a pure breach of contract case, where a defendant's conduct does not give rise to separate liability in tort, the public policy rule prohibiting parties from immunizing themselves from liability for grossly negligent conduct applies only to exculpatory or nominal damages clauses.”). Additionally, attempts to limit liability in tort for gross negligence and willful conduct are unenforceable. *See Gross v. Sweet*, 400 N.E.2d 306, 308 (N.Y. 1979) (noting that an exculpatory clause cannot reach “liability for willful or grossly negligent acts”). The Court need not address that issue now, because Plaintiff's Count VII seeks a declaration that the provision is unenforceable and not that it is inapplicable to a claim of gross negligence.

¹⁷ Plaintiff does not request leave to replead and does not “identify [any] additional facts or legal theories that [he] might assert if given the opportunity to replead. For this reason and because the Court concludes that any amendment,” of Counts I and VII of the Complaint are dismissed with prejudice. *Wade Park Land Holdings, LLC v. Kalikow*, 589 F. Supp. 3d 335, 401 (S.D.N.Y. 2022), *amended*, 2022 WL 2479110 (S.D.N.Y. July 6, 2022). However, the Court dismisses Counts II and IV without prejudice.

¹⁸ Defendant also moves to dismiss Count III (Plaintiff's MCPA claim) on the grounds that the choice-of-law provision in the Terms and Conditions precludes Plaintiff from relying on the MCPA. Dkt. No. 20 at 4–5. Plaintiff argues that “Uphold has not offered any argument that the choice of law clause can overcome Plaintiff's right to assert a claim under the MCPA, a remedial statute designed to protect Michigan consumers like Yuille.” Dkt. No. 23 at 18. The motion is denied without prejudice to renewal of the motion against the MCPA claim after Plaintiff has amended his Complaint, or, if Plaintiff does not amend his Complaint, forty-five days from the date of this Opinion and Order, on the grounds set forth in the current motion or any other available arguments.

The current motion raises the issue whether a party who was precluded from bringing a claim under the NYGBL because he did not purchase the product in New York, could also be

The Clerk of Court is respectfully directed to close Dkt. No. 18.

SO ORDERED.

Dated: August 11, 2023
New York, New York



LEWIS J. LIMAN
United States District Judge

precluded from bringing a claim under the consumer protection laws of the State in which the party made the purchase by virtue of a contractual choice-of-law provision stipulating that New York law would govern the relationship between the parties. The Terms and Conditions contain a choice-of-law provision that the parties agreed to when Yuille signed up for the Account. That provision reads: “You agree that the laws of the State of New York, without regard to principles of conflict of laws, govern these Terms and Conditions and any claim or dispute between you and us except to the extent governed by U.S. federal law.” Dkt. No. 19-1 § 13.8. A “district court . . . , sitting in diversity, [is] bound to apply New York law to determine the scope of the contractual choice-of-law clause. New York courts decide the scope of such clauses under New York law, not under the law selected by the clause, which here also happens to be New York law.” *Fin. One Pub. Co. v. Lehman Bros. Special Fin.*, 414 F.3d 325, 333 (2d Cir. 2005). “New York courts are ‘reluctant to read choice-of-law clauses broadly.’” *Arnone v. Aetna Life Ins. Co.*, 860 F.3d 97, 108 (2d Cir. 2017) (alterations adopted) (quoting *Fin. One Pub. Co.*, 414 F.3d at 332, 335). Specifically, there is “a reluctance on the part of New York courts to construe contractual choice-of-law clauses broadly to encompass extra-contractual causes of action.” *Fin. One Pub. Co.*, 414 F.3d at 334.

However, under New York law, “where the ‘express language’ of a choice-of-law provision is ‘sufficiently broad as to encompass the entire relationship between the contracting parties,’ New York law will ‘apply [that provision] to claims for tort arising incident to the contract.’” *Ramiro Aviles v. S & P Glob., Inc.*, 380 F. Supp. 3d 221, 270 (S.D.N.Y. 2019) (quoting *Krock v. Lipsay*, 97 F.3d 640, 645 (2d Cir. 1996)); *see also Fin. One Public Co.*, 414 F.3d at 335 (noting that “a contractual choice-of-law clause could be drafted broadly enough to reach . . . tort claims”); *Turtur v. Rothschild Registry Int’l, Inc.*, 26 F.3d 304, 310 (2d Cir. 1994) (holding that a New York choice-of-law clause applying to “any controversy ‘arising out of or relating to’” the agreement was “sufficiently broad to cover” fraud claim arising out of and related to the agreement). Defendant thus argues that the choice of law clause in the Terms and Conditions is broad enough reach statutory claims. The parties have cited no binding authority addressing the question whether such a clause would prohibit the consumer from bringing a claim under a consumer protection statute, much less under circumstances where the effect of a Defendant’s reading of the clause would be to deprive the consumer of the protection of any consumer protection statute. *Cf. Miramontes v. Ralph Lauren Corp.*, 2023 WL 3293424, at *7 (S.D.N.Y. May 5, 2023) (noting that several consumer protection “statutes contain language indicating that they are designed to protect the citizens of a particular state from deceptive practices in the state”). Accordingly, Defendant’s motion to dismiss Count III is denied without prejudice to renewal.