SUPREME COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY

PRESENT: HON. PHAEDRA F. PERRY-BOND PART 35

Justice

---X

PEOPLE OF THE STATE OF NEW YORK, BY LETITIA JAMES, ATTORNEY GENERAL OF THE STATE OF NEW YORK,

Plaintiff,

- v -

EARLY WARNING SERVICES, LLC,

Defendant.

---X

INDEX NO. 654753/2025

MOTION DATE 04/10/2026

MOTION SEQ. NO. 008

DECISION + ORDER ON MOTION

The following e-filed documents, listed by NYSCEF document number (Motion 008) 76, 77, 78, 79, 80, 81, 86, 89

were read on this motion to/for DISMISS.

Upon the foregoing documents, and after oral argument, which took place on July 7, 2026, defendant Early Warning Services, LLC's ("Defendant") motion to dismiss plaintiff the People of the State of New York, by Letitia James, Attorney General of the State of New York (the "OAG") is denied.

I. Background

Digital interactions are expanding exponentially into our everyday lives. As technology progresses and proliferates, the boundaries between the material and digital worlds continuously wane. The creation and expansion of digital networks are immensely beneficial for efficiency, convenience, and interconnectivity. However, in racing to create the most efficient and innovative technologies, consumer safety is sometimes deprioritized. Examples throughout history demonstrate some are willing to risk liability for harming consumers to ensure a new product or service saturates the market and becomes ingrained in everyday life as quickly as possible.

The exponential rise in digital interactions, coupled with rapidly advancing technology, is enabling increasingly sophisticated fraudulent schemes to be perpetrated via new digital platforms and technology. Striking a balance between technological innovation and consumer protection is more important now than ever, especially where artificial intelligence can create startlingly convincing "deepfakes" of individuals. Society requires all available tools to protect and educate consumers, to ensure developers can remedy design flaws in their technologies, platforms, and applications, and to hold developers accountable when they fail to take reasonable measures to remediate identifiable dangerous design flaws.

New York's legislature recognizes the importance of creating powerful tools to protect consumers, which is why it enacted Executive Law § 63(12) many years ago. This lawsuit is novel in that the OAG seeks to apply Executive Law § 63(12) to a newly created digital payment network. However, the allegations at their core state a repeated narrative: a product or service is developed and distributed, the company learns of the product's dangers (here, the platform's design allegedly made it inherently prone to fraudulent outcomes), and the company declines to mitigate those dangers due to prioritizing profit and market dominance. The following decision provides the reasoning and analysis as to why the OAG's complaint should not be dismissed prior to Defendant answering the allegations and testing those allegations' veracity through discovery.

A. Defendant's Inception and Zelle's Implementation

Defendant, an entity created by some of the largest banks in the United States[1], developed and owns the FinTech application known as Zelle. In January 2016, Defendant announced its intention to build a digital payments network that would form "the largest, most secure real-time payments ecosystem in the U.S." At this time, the digital payments market was dominated by

[1] Defendant is allegedly owned by Bank of America, N.A., Capital One, N.A., JPMorgan Chase Bank, N.A., PNC Bank, N.A., Truist Bank, Wells Fargo Bank, N.A., and U.S. Bank, N.A.

electronic payment applications that were not linked to the banks, such as PayPal and Venmo. The OAG alleges Zelle's development and implementation was rushed due to the Defendant's desire to compete for market share in the digital payment market.

It is further alleged that to obtain the greatest amount of market share, Defendant designed Zelle's infrastructure in the most simple and accessible manner possible. To this end, Zelle was designed so that money was instantly transferred from one user's bank account to another user's bank account. This was a significant advantage over competitors such as Venmo and Cash App, which did not have the network or partnership with banks to allow for instant money transfers.

Defendant developed a network capable of instantaneous digital fund transfers by creating a partnership network with over 2,200 banks. Defendant established a management committee to promulgate rules governing money transfers between participating banks, users, and Defendant. The network was designed such that enforcement of the network's rules was left solely to Defendant, and Defendant could assess fees against partner banks who were noncompliant with the rules. The network's rules allegedly included requirements for partner banks to report, respond to, and reimburse consumers for fraud-based losses arising from Zelle's digital network.

Defendant made registering for Zelle exceedingly simple. Zelle only required an email address or mobile number, and a bank account or debit card associated with one of the banks partnered with Zelle. The design was such that one person could make multiple Zelle accounts by using multiple e-mail addresses or mobile numbers. All that was required to validate an account was for a user to enter a passcode delivered to the user's e-mail address or mobile number.

Zelle tried to attract consumers by representing it was safe and secure due to its association with banks. Specifically, Zelle advertised itself by stating it was "backed by the banks, so you know its secure" and telling consumers they could "safely send and receive money straight from your banking app." The advertisements were buttressed by Defendant and partner banks embedding Zelle within mobile banking applications.

B. Defendant's Knowledge that Zelle's Design was Conducive to Fraud

The OAG alleges that Zelle's design, advertising, lack of enforcement of network rules, and insufficient verification in the account registration process made it attractive to fraudsters. Zelle's focus on making transferred funds immediately available in a user's bank account allowed fraudsters to quickly dissipate fraudulently obtained money, making consumers' chance of recovery slim to none. Moreover, because funds were made available in almost real time, completed transfers were irrevocable. Allegedly, Zelle's design and network rules made it possible for one user to register more than five Zelle accounts at a time. Zelle's simple registration process, which allowed one person to create multiple accounts using multiple e-mail addresses, allowed fraudsters to create many accounts using fraudulent e-mail addresses which easily tricked unassuming consumers. The simple registration process turned tackling fraudsters into a game of whack-a-mole. If one account was shut down, nothing prevented the fraudster from re-registering using a different e-mail.

The OAG alleges that based on Zelle's design, its emphasis on efficiency and accessibility, and advertisements that Zelle was safer and more secure due to its connection to the banks, fraud rapidly proliferated on Defendant's digital payment network. Allegedly, within Zelle's first year of launching, one large bank found fraud attack rates of 25.12% for transfers compared to an attack rate of .736% for a major competitor's network. Defendant's internal memoranda admitted to a 30% attack rate at Zelle's launch, which remained at 7-10% attack rates months after launch.

The fraud perpetrated on Zelle manifested in various forms. One form was induced fraud, also known as scams. These scams included a variety of schemes, including fraudsters impersonating banks, governments, or merchants. Because the registration process required almost no verification of a user's identity, scam victims had no means of learning the identity of the scam's perpetrator. Fraudsters were permitted to register with misleading e-mail addresses closely linked to banks or government entities. Despite knowledge of the issue of misleading e-mails, Defendant did nothing to limit the ability to register with suspicious or misleading e-mail addresses. Further, the user transferring funds was provided with minimal information about the recipient of those funds prior to effectuating the transfer. Often, the only information shown prior to transfer was the recipient's first name, which made it difficult for scam victims to recognize they were sending money to an imposter.

Defendant allegedly tried to conceal the amount of induced fraud or was willfully ignoring it. Defendant's network rules allegedly did not require partner banks to report induced fraud. When Defendant eventually changed this rule, partner banks were permitted to report induced fraud weeks after the fraud was committed which allowed fraudsters to continue defrauding consumers for lengthy amounts of time.

C. Defendant Declines to Implement Safeguards Despite Knowledge of Fraud Proliferating on Zelle

The OAG alleges that although Defendant could, within its network rules, set parameters for suspicious or risky transactions, they failed to define specific thresholds, characteristics, or factors that would create an obligation for partner banks to pause or block certain transfers. The OAG alleges that Defendant's own internal audit assigned its anti-fraud team consistent "unsatisfactory" ratings for failing to detect and limit fraud. By July 2019, Defendant allegedly developed basic safeguards to help identify fraudsters and ensure their swift and permanent removal from the network. These safeguards included a requirement for partner banks to share reports of fraud with Defendant immediately and proposed delegating responsibility to partner banks in making whole certain victims of induced fraud. Defendant also proposed automatic restrictions of a user from Zelle upon two or more unique reports of fraud associated with that user.

When presented with these proposed changes, the partner banks objected. Defendant acquiesced to the partner banks' objections to consumers' detriment. Instead of implementing identified safeguards, Defendant's network rules in late 2019 required accounts to be restricted only after an investigation into alleged fraud, which could take weeks. If partner banks wished to do so, they could reinstate accounts previously restricted for fraud. Finally, Defendant implemented a "scam fee" consisting of a $2,500 fine to be imposed if a partner bank reinstated a previously restricted account and that account was again reported for fraud after reinstatement. Allegedly, this scam fee was rarely enforced, and even when enforced, was a meaningless deterrent because of how small the fine was in comparison to the assets of the banks against whom the penalty was levied. Allegedly, even when fines were imposed, they were often waived or refunded.

Allegedly, due to Defendant's failure to remedy Defendant's self-identified flaws, fraud grew more rampant on Zelle's network. Defendant allegedly received 150,000 reports of induced fraud in 2020 with losses of $80 million. In 2021, Defendant received 375,000 reports of fraudulent transfers with internal estimates of $213.5 million in losses. In 2022, Defendant estimated $500 million in consumer losses to fraud perpetrated through Zelle, with $300 million attributable to induced fraud. Meanwhile, Defendant was profiting from transfer fees related to these fraudulent transfers and was keeping partner banks engaged due to lax rules with minimal penalties.

D. Federal Investigations, Implementation of Safeguards, and Federal Lawsuit

By 2022, Zelle became the largest payment to payment network within the United States. Only in June of 2023, after investigations and reports issued by Congress, and an investigation by the Consumer Financial Protection Bureau ("CFPB"), did Defendant begin implementing the safeguards it originally proposed to partner banks in 2019. Upon implementation, Defendant reported a substantial decrease in consumer losses attributable to reported fraud. CFPB's investigation led to a lawsuit filed against Defendant on December 20, 2024. But on January 31, 2025, upon a change in administration, the CFPB director was fired. On March 4, 2025, CFPB voluntarily discontinued its lawsuit with prejudice and without explanation. Prior to the voluntary dismissal, Defendant never responded to that lawsuit.

E. This Lawsuit and the Motion to Dismiss

The OAG filed this lawsuit on August 12, 2025, alleging Defendant violated Executive Law § 63(12). The OAG alleges Defendant created an atmosphere conducive to fraud by creating a digital payment network integrated into consumers' banking apps, and notwithstanding Defendant's knowledge of widespread fraud taking place on Defendant's network and ability to mitigate fraud, Defendant chose to appease partner banks and expand market dominance rather than designing fraud off of its network. The OAG further argues the failure to enforce its own network rules exacerbated an atmosphere already conducive to fraud. The OAG also alleges Executive Law § 63(12) was violated because Defendant knew Zelle was neither safe nor secure from fraudsters and knew consumer losses from induced fraud would not be "backed by the banks" yet deceptively advertised Zelle as being safe and secure because it was backed by banks. As remedies for the alleged violations of Executive Law § 63(12), the OAG seeks, *inter alis*, an injunction requiring Defendant to maintain basic network safeguards and other necessary antifraud measures, an accounting of New York consumers who reported losses to Defendant, restitution, disgorgement of profits obtained through fraudulent practices, and costs.

On September 12, 2025, Defendant removed this matter to the United States District Court for the Southern District of New York ("SDNY"). Defendant argued SDNY could exercise federal-question jurisdiction over the Executive Law § 63(12) claim because it was premised on violations of federal law, specifically the Consumer Financial Protection Act ("CFPA") (*see* 12 USC § 5481 *et seq.*) and the Electronic Funds Transfer Act ("EFTA") (*see* 15 USC § 1693 *et seq.*). However, in an amended decision and order dated February 26, 2026, United States District Judge Margaret M. Garnett remanded this action back to this Court. Judge Garnett found the OAG's claim does not turn on a question of federal law and could be resolved solely through an adjudication as to whether Defendant committed fraud within the meaning of Executive Law § 63(12) (*see New York v Early Warning Services, LLC*, 2026 WL 570793 at *3 [SDNY 2026]).

Upon remand, Defendant filed this motion to dismiss. Defendant argues that advertising Zelle as safe and secure was neither false nor misleading and could not be interpreted to promise immunity from third-party fraud. Defendant claims the advertised statements are true or amount to nonactionable opinions. Defendant further argues that Executive Law § 63(12) must be interpreted against a background of common-law principles, and applying those principles to the allegations, Defendant cannot be liable for creating an atmosphere conducive to fraud. Defendant argues it cannot be liable because it did not knowingly and actively participate in fraud, nor is it responsible for another's fraud under any theory of agency. Defendant claims it cannot be held liable for its own passive nonfeasance. Defendant then argues that the relief and damages sought is improper. *Amici curiae* submitted a brief in support of the motion to dismiss which mainly offers public policy arguments against the relief sought by the OAG.

In opposition, the OAG argues Defendant misinterprets and misapplies Executive Law § 63(12), which was drafted to provide a broad and remedial tool to root out fraud in New York.

The OAG argues that contrary to Defendant's attempt to apply principles of common law, in enacting Executive Law § 63(12) the legislature overrode the common law to create a statutory remedy for certain kinds of fraudulent practices common law fraud was unable to address. The OAG also argues Defendant's cited cases have nothing to do with the statute or facts alleged here, noting Defendant overly relies on out-of-state, private-party actions based on common-law fraud claims. The OAG further argues that under binding First Department law, a defendant can be held liable for creating an atmosphere conducive to fraud even in the absence of an agency relationship. The OAG also argues Defendant misconstrues the complaint. The OAG claims Defendant is not sued for third-party fraud but is sued for creating an easily exploitable payment network, recognizing the exploitable features of that network, identifying rampant fraud occurring due to the network's flaws, and choosing to leave those flaws unaddressed at consumers' expense in order appease partner banks whose participation was necessary for the existence of the network.

The OAG argues that Defendant's claim that the volume of frauds or scams was small is without merit because it is alleged Defendant's design and maintenance of Zelle caused consumers to lose more than one billion dollars to fraudulent activity and is further alleged fraud was under-reported and under-investigated. The OAG argues that the test as to whether there was deceptive marketing is context dependent and relies on whether the marketing gave consumers a net impression that was misleading. Finally, the OAG argues the Court should decline to entertain a limitation of remedies or damages at the pre-answer motion to dismiss stage.

II. Discussion

A. Standard

When reviewing a pre-answer motion to dismiss for failure to state a claim, the Court accepts all factual allegations as true, gives claimant the benefit of all favorable inferences which may be drawn from the pleadings, and determines only whether the alleged facts fit within any cognizable legal theory (*Sassi v Mobile Life Support Services, Inc.*, 37 NY3d 236, 239 [2021]). The sole criterion for a Court to determine on a motion to dismiss for failure to state a claim is whether the pleadings, read holistically within its four corners, manifests any cause of action cognizable at law (*African Diaspora Maritime Corp. v Golden Gate Yacht Club*, 109 AD3d 204 [1st Dept 2013]).

Executive Law § 63(12) provides:

> "Whenever any person shall engage in repeated fraudulent or illegal acts or otherwise demonstrate persistent fraud or illegality in the carrying on, conducting or transaction of business, the attorney general may apply, in the name of the people of the state of New York, to the supreme court of the state of New York, on notice of five days, for an order enjoining the continuance of such business activity or of any fraudulent or illegal acts, directing restitution and damages… ."

The statute defines "fraud" as "any device, scheme or artifice to defraud and any deception, misrepresentation, concealment, suppression, false pretense, false promise or unconscionable contractual provisions." The statute further provides that "'persistent fraud' or 'illegality' as used herein shall include continuance or carrying on of any fraudulent or illegal act or conduct."

To allege a violation of Executive Law § 63(12), there must be facts showing the defendant had "the capacity or tendency to deceive or create[d] an atmosphere conducive to fraud" (*People v General Elec. Co.,* 302 AD2d 314, 314 [1st Dept 2003]). "Executive Law § 63(12) was meant to protect not only the average consumer, but also the ignorant, the unthinking, and the credulous" (*see People v Northern Leasing Systems, Inc.*, 193 AD3d 67, 75 [1st Dept 2021], *lv dismissed*, 37 NY3d 1088 [2021]). "[T]he statute does not require proof of all the elements of common-law fraud" (*see People v Trump*, 249 AD3d 21, 28 [1st Dept 2025] [Moulton, J. concurring]). "[W]hether a counterparty exercised due diligence or justifiably relied on the fraudulent conduct" is not required to establish fraud or fraudulent acts within the meaning of Executive Law § 63(12) (*id.* at 59). Moreover, allegations of reports of fraud, whether public or internal, are enough to draw a rational inference of actual knowledge of the fraud and raise an issue of fact as to scienter (*Northern Leasing, supra* at 75).

A defendant creates an "atmosphere conducive to fraud" where (1) a defendant creates a market, or provides certain goods or services (2) the defendant learns of ongoing fraud being perpetrated on the public through the use of the market, goods, or services created by defendant; (3) the defendant does nothing to remedy the ongoing fraud to the public's detriment, and (4) the defendant expressly or implicitly ratifies the ongoing fraud (*see Northern Leasing,* at 75-76). This includes the failure to perform any procedures to verify the accuracy of information injected into the market, which results in the unverified and deceptive information causing injury to members of the public (*People v Trump* at 65). An absence of an agency relationship between the creator of the market, goods, or services and the parties using that market or those goods and services to perpetrate fraud is not fatal to an Executive Law § 63(12) claim (*Northern leasing* at 76). Benefitting from unauthorized transactions, despite knowledge of the fraudulent nature of the transaction, is sufficient to allege that a defendant created an atmosphere conducive to fraud (*id.*).

As a remedial statute which supplies the OAG with a new remedy not available at common law, Executive Law § 63(12) must be liberally construed to spread its beneficial effects as widely as possible (*see generally People v Brown*, 25 NY3d 247, 251 [2015] quoting McKinney's Cons. Laws of NY, Book 1, Statutes § 321 ["generally, remedial statutes are liberally construed to carry out the reforms intended and to promote justice"]). In interpreting and applying Executive Law § 63(12), it is not for the courts "to determine the wisdom of economic oversight and intervention allowed by the Legislature, so long as such interventions do not run afoul of the state or federal constitutions" (*People v Trump*, at 41).

B. Violation Predicated on Defendant's Fraudulent Conduct in Marketing of Zelle

The motion to dismiss the branch of the Executive Law § 63(12) claim predicated on alleged fraudulent marketing of Zelle is denied. Accepting the allegations as true, and drawing all favorable inferences in favor of the OAG, as this Court must on a pre-answer motion to dismiss, the OAG adequately alleged that Defendant knowingly made statements when marketing Zelle which had "the capacity or tendency to deceive" both "the credulous and unthinking consumer" as well as the suspicious and cynical consumer (*see People v General Elec. Co.*, 302 AD2d 314, 314 [1st Dept 2003] citing *Guggenheimer v Ginzberg*, 43 NY2d 268, 273 [1977]).

The alleged context in which Zelle was marketed is important. Unlike Zelle's competitors, Zelle was automatically embedded in consumer's mobile banking applications, giving the impression that Zelle was not operated by a separate entity but was an extension of the bank. Defendant knowingly leveraged its connection to the banks to lure users to Zelle. Defendant told consumers that Zelle was "backed by the banks, so you know its secure" and that consumers could "send and receive money fast – all with the peace-of-mind that your transactions will be backed by the security of your trusted financial institution." But the complaint alleges that Defendant knew consumers would not be "backed by the banks" if they fell victim to induced fraud. And Defendant knew Zelle was not safe because hundreds of millions of dollars were being lost by consumers because fraudsters could simply re-register for Zelle even when one of their accounts was banned. Defendant also misled consumers that it was secure to "send and receive money fast" when it is alleged that the instantaneous transfer of money meant consumers were often left without recourse as fraudsters could quickly dissipate transferred funds, and transfers were made irrevocable.

That some language in advertisements may be considered in isolation as "puffery" is of no moment where other statements in advertisements are actionable; the allegedly deceptive advertising must be reviewed holistically to determine the net impact on the consumer (*see People v Charter Communications, Inc.*, 162 AD3d 553, 554 [1st Dept 2018]). Moreover, whether Defendant provided users with disclaimers is not dispositive at this stage, where the disclaimers were neither sufficiently prominent nor clear to negate the alleged overall misleading advertisements to consumers (*see People v Orbital Publishing Group, Inc.*, 169 AD3d 564, 566 [1st Dept 2019]). The non-binding and distinguishable out of state or federal district court cases relied upon by Defendant are unavailing, at least at this juncture. Given this is a pre-answer motion to dismiss, considering the detailed allegations, and because the full advertising content is not included in the record, Defendant's motion to dismiss the Executive Law § 63(12) claim predicated on alleged fraudulent marketing of Zelle is denied.

C. Violation Predicated on Creating an Atmosphere Conducive to Fraud

The motion to dismiss the branch of the Executive Law § 63(12) claim predicated on creating an atmosphere conducive to fraud is also denied. It is alleged with specificity that Defendant rushed the design, marketing, and implementation of Zelle and prioritized accessibility, convenience, consumer adoption, and market dominance at the expense of consumer safety. Although Defendant was aware of the design deficiencies and developed network rules to design fraud out of Zelle's network, it allegedly chose not to do so after facing objections from its partner banks. Allegedly, as the network operator who promulgated and enforced the network's rules, Defendant had the final say as to what rules and safeguards were in place. Yet, for years Defendant allegedly decided to do next to nothing as consumers lost exorbitant sums to fraudulent schemes each year.

As recently held by the First Department, even in the absence of an agency relationship, an atmosphere conducive to fraud can be created where the creator of the enterprise fails to enforce any meaningful penalty against individuals they know are committing fraud through the enterprise, thereby allowing fraud to be perpetrated continuously and systemically (*see People v Northern Leasing Systems, Inc.*, 193 AD3d 67, 75 [1st Dept 2021]). Here, it is alleged that Defendant failed to assess even minimal penalties against banks who were violating network rules by failing to report and investigate fraud. Moreover, fraudsters were allowed to remain on Zelle while being investigated. Even when one account was deplatformed, the fraudster could simply make a new account with a different e-mail or mobile phone number, thereby allowing fraud to go unchecked.

It is also alleged that Defendant allowed Zelle to become permeated with fraudsters using blatantly deceptive and misleading e-mail addresses despite Defendant's alleged ability to prevent this practice. It is alleged Defendant knowingly allowed users to register with e-mails mimicking governmental entities, banks, or utility service providers which were used to scam consumers via Zelle. The failure to conduct any sort of verification of a user's identity, coupled with the use of misleading e-mails and imposters posing as banks, companies, or the government, created an atmosphere conducive to fraud (*see People v Trump*, 249 AD3d 21, 65-66 [1st Dept 2025] [Moulton, J., concurring] [atmosphere conducive to fraud created where accountants failed to perform any procedures to verify the accuracy or completeness of the information provided]). Defendant's design of the digital payment network and failure to implement safeguards despite identifying serious design flaws allowed fraudsters to conceal their true identities thereby defrauding consumers and making investigations into fraud that much more difficult (*id.* at 65-66).

Defendant's argument that it did not ratify or benefit from any fraud is unavailing on this pre-answer motion to dismiss. Despite knowledge of hundreds of millions of dollars being lost to fraudulent schemes effectuated via Zelle, it is alleged, and Defendant conceded at oral argument, that Defendant continued to collect and retain transaction fees from those fraudulent transactions.

At a minimum, this creates an issue of fact on this pre-answer motion to dismiss as to whether Defendant implicitly or expressly ratified the fraudsters' actions. Moreover, express or implied ratification is alleged because the OAG claims Defendant did nothing to stop the allegedly growing fraudulent transactions due to Defendant's desire to appease partner banks, who objected to proposed changes to the network rules, rather than implementing safeguards for consumers. Implied ratification is further alleged because Defendant failed to assess penalties against banks who were violating network rules by failing to report and investigate fraud, raising an issue of fact as to whether Defendant implicitly condoned the existence of fraud on its network.

Defendant's argument that "fraud was not committed on Zelle's network" is without merit as it was through Zelle's network that the fraud was effectuated and the consumer was damaged. The case law relied upon by Defendant is likewise unavailing, unpersuasive, and non-binding. Defendant's cases are also easily distinguishable, as the cases stressed the most by Defendant do not even deal with Executive Law § 63(12) claims. Defendant's argument that the fraud was *de minimis* is unavailing. It is alleged the fraud resulted in almost $1 billion dollars of consumer losses, which is not a *de minimis* amount. It is likewise irrelevant that the challenged acts and practices have since been changed as there may still be a finding of liability for the years the safeguards were identified but not implemented (*see People v Orbital Publishing Group, Inc.*, 169 AD3d 564 565 [1st Dept 2019]). Therefore, the motion to dismiss the Executive Law § 63(12) claim predicated on Defendant allegedly creating an atmosphere conducive to fraud is denied.

D. Damages & Public Policy Arguments

At this pre-discovery stage the Court finds it premature to dismiss the OAG's requested remedies. There has not yet been any discovery and therefore it would be inappropriate for this Court to determine what remedies and damages may ultimately be available (*see generally Island*

Consolidated v Grassi & Co., 239 AD3d 443, 444-445 [1st Dept 2025]). Moreover, the public policy arguments made by *amici curiae* are premature and provide no basis to grant dismissal since there is not yet any finding of liability against Defendant. The Court has considered the remainder of Defendant's contentions and at this juncture finds them unavailing.

Accordingly, it is hereby,

ORDERED that the motion to dismiss is denied in its entirety, and within twenty days of entry, counsel for Defendant shall serve an answer to the complaint; and it is further

ORDERED that on or before September 8, 2026, the parties shall meet and confer and submit a proposed preliminary conference order or, if the parties believe discovery in this case requires a discovery referee, shall submit lists of proposed discovery referees to oversee discovery in this matter. If the parties believe a discovery referee is needed but cannot agree on one, the Court shall appoint one unilaterally; and it is further

ORDERED that within ten days of entry, counsel for the OAG shall serve a copy of this Decision and Order, with notice of entry, on all parties via NYSCEF.

This constitutes the Decision and Order of the Court.

7/20/26
DATE

HON. PHAEDRA F. PERRY-BOND, J.S.C.

CHECK ONE:	☐ CASE DISPOSED		☒ NON-FINAL DISPOSITION	
	☐ GRANTED	☒ DENIED	☐ GRANTED IN PART	☐ OTHER
APPLICATION:	☐ SETTLE ORDER		☐ SUBMIT ORDER	
CHECK IF APPROPRIATE:	☐ INCLUDES TRANSFER/REASSIGN		☐ FIDUCIARY APPOINTMENT	☐ REFERENCE