In this Issue: Fraud

The Deepfake and the Algorithm: Intent, Loss, and New Jersey’s Two Tracks for AI Fraud

Asaad K. Siddiqi and Luke D. Grygier

I. The Two Tracks New Jersey Has Built

A cloned voice authorizes a wire transfer no partner ever approved. Two shoppers check out side by side and pay two different prices for the same carton of eggs, because an algorithm priced each of them separately. New Jersey has no omnibus statute governing the specific use of artificial intelligence in either scenario, and none is on the horizon.

Since the spring of 2025 the state Legislature has instead been regulating machine-generated deception along two separate tracks, one criminal and one consumer, drafted by different sponsors, lodged in different code titles, and organized around different theories of harm. Each track has now produced something concrete, an enacted deep-fake statute on the criminal side and, on the consumer side, a pricing bill that passed both Houses at the end of June and sits on the governor's desk. A lawyer who wants to know whether artificial intelligence-enabled conduct is actionable in New Jersey starts with a sorting question: which track does the conduct fall on?

The criminal track came first. In April 2025, Gov. Phil Murphy signed P.L. 2025, c.40, which supplements the criminal code and makes it a crime of the third degree to create a work of deceptive audio or visual media, the statute's term for a deep-fake, for the purpose of furthering any crime or offense, with parallel offenses for soliciting, disclosing, or using such a work and fines of up to $30,000.1 The act gives victims a civil action in the Superior Court, with liquidated damages, punitive damages, fee-shifting, and no requirement of a prior conviction.2 It writes its First Amendment accommodations directly into the text, exempting content a reasonable viewer would take as criticism, comment, satire, parody, news reporting, teaching, scholarship, or research, along with the service providers and AI developers whose infrastructure the media passes through.3 Subsequent legislative efforts point in the same direction. S. 3303 would extend the voyeurism and nonconsensual-disclosure crimes to AI-generated images.4 A. 3058 would establish a Deepfake Technology Unit in the Department of Law and Public

Safety with a $2 million appropriation.5 Federally, the TAKE IT DOWN Act criminalizes the nonconsensual publication of intimate visual depictions, including digital forgeries, and, since May 19, 2026, requires covered platforms to operate a notice-and-removal process.6 The consumer track runs through the Consumer Fraud Act. The Fair Price Protection Act, which passed both Houses on June 30, 2026, and now awaits Gov. Mikie Sherrill's signature, supplements the CFA directly and bars grocery stores and third-party delivery platforms from using algorithms to set individualized prices for particular shoppers.7

The governor has signaled she will sign it, and if she does, New Jersey becomes the third state to restrict personalized pricing, behind Maryland and Connecticut, with New York's bill awaiting the governor's signature in Albany.8 There are additional bills taking the same route. S. 3952 would reach surveillance and dynamic pricing in grocery sales and impose a moratorium on electronic shelf labels in larger stores.[9] A. 3989 would carry the prohibition against algorithmic pricing into residential rentals.[10] None of these builds a new enforcement system. Each drops a freshly prohibited practice into a statute that has policed the marketplace since 1960. The difficult question raised by these new laws is whether the CFA's full remedial arsenal follows, including the private right of action, the treble damages, and the mandatory fee award.[11]

The two tracks divide along a line that looks administrative and is actually doctrinal. A deepfake used to defraud is rarely part of a consumer transaction, so it sits in the criminal code. A pricing algorithm operates inside a sale, so it sits in the CFA. That sorting decision fixes everything downstream. The criminal track turns on intent, which the CFA's strict-liability lane was built to avoid.

The consumer track for a private plaintiff turns on ascertainable loss, which the criminal law never asks about. Part II examines the consumer track and shows that the Consumer Fraud Act handles one kind of algorithmic conduct well and another not at all. Part III examines the criminal track and its blind spots. Part IV proposes what a Legislature this active should take up next.

II. The Consumer Fraud Act and Two Kinds of Algorithmic Conduct

Artificial intelligence poses two distinct problems for the Consumer Fraud Act. One is algorithmic personalized pricing, which the statute in its present form does not reach. That is why the Legislature has set out to prohibit it by name. The other is the use of AI to carry out ordinary deception, which the statute has prohibited since 1960 and reaches today without amendment. Treating both as a single category of “AI fraud” obscures what is new about each. What separates them is loss. Each theory rises or falls on whether the consumer can show an injury the statute recognizes.

A. The architecture: three categories and a separate loss requirement

The CFA sorts unlawful practices into three categories: affirmative acts, knowing omissions, and regulatory violations.12 Intent works differently in each. A plaintiff who alleges an affirmative misrepresentation need not prove that the defendant intended to commit an unlawful act.13 A plaintiff who alleges an omission must prove knowledge, so intent is an element of the claim.14 A plaintiff who alleges the violation of a regulation adopted under the act need not prove intent at all, because those violations carry strict liability.15

That last category does most of the work in an algorithmic case. The recurring difficulty with an automated system is locating intent. A business that deploys a pricing model forms no state of mind toward any particular shopper, and the model has none of its own. An omission theory fails for the same reason. Only the strict-liability category fits a personalized-pricing claim, and it is the category the Legislature’s pricing measures have chosen.

In addition to proving an unlawful practice, a private plaintiff must also establish an ascertainable loss and a causal link between the violation and that loss.16 The loss element stands on its own, and it is unforgiving. The loss must be quantifiable or measurable, not hypothetical or illusory.17 A plaintiff who offers no evidence of a measurable loss will lose at summary judgment, however plain the violation.18

Two features of the loss requirement shape everything that follows. First, it binds private plaintiffs only. The ascertainable loss requirement is a prerequisite for a private cause of action; it does not constrain an enforcement action brought by the Attorney General.19 Whether the loss requirement applies can therefore turn on nothing more than the identity of the plaintiff. Second, the New Jersey Supreme Court raised the bar in 2024. In *Robey v. SPARC Group, LLC,* the Court held that shoppers who bought conforming, non-defective goods at an agreed price suffered no ascertainable loss, even though the advertised discount was illusory because the reference price was fictitious. The shoppers got what they paid for, and no measurable gap separated what they expected from what they received.20 The Court closed off the fallback as well, holding that a consumer without an ascertainable loss is not an aggrieved consumer under the Truth-in-Consumer Contract, Warranty, and Notice Act.21

B. Theory One: personalized pricing as a per se wrong beyond the statute's current reach

---

A common assumption is that surveillance pricing already violates the CFA because the statute supposedly requires one fixed price on the shelf.

It does not. Nothing in the CFA imposes a general one-price rule or forbids a seller from charging two customers different amounts for the same item.

A common assumption is that surveillance pricing already violates the CFA because the statute supposedly requires one fixed price on the shelf. It does not. Nothing in the CFA imposes a general one-price rule or forbids a seller from charging two customers different amounts for the same item. Charging one shopper more because an algorithm predicts she will tolerate it is not, standing alone, a misrepresentation. The price she pays is the price she agreed to and it is not a regulatory violation without a regulation on point. The federal statute aimed at price discrimination, the Robinson-Patman Act, is antitrust law that protects competing merchants, not retail consumers, and it is rarely enforced today. It is not the consumer's vehicle.

What the CFA does require is a posted price. Section 56:8-2.5 makes it an unlawful practice to offer merchandise for retail sale unless the total selling price is plainly marked by a stamp, tag, label, or sign.22 The unit-pricing statutes and their regulations rest on the same premise, that a shopper can read one publicly displayed price and weigh it against the alternatives.23 The plaintiffs in *Dugan v. TGI Fridays,* Inc., both the *Dugan* and *Bozzi* claimants, built their regulatory-violation theory on this very provision, arguing that a restaurant's failure to print drink prices violated Section 56:8-2.5.24

This is where the doctrine turns. Every one of the CFA's pricing rules assumes a price that sits in public view and stays put. Personalized and dynamic pricing attacks that premise at its root. There is no settled, plainly marked price, because the price is computed for the individual in real time and can change within minutes or from one transaction to the next.25 Electronic shelf labels make even the displayed number something that moves. The wrong addressed by older rules is a missing or inaccurate posted price. The wrong now emerging is an individualized price with no public reference point at all. The statute as written catches the first and not the second.

The best evidence that current law does not reach personalized pricing is the bill written to capture it. If surveillance pricing already qualified as an unlawful practice, there would be no need for the Fair Price Protection Act to declare that it does.26 The legislation exists because the conduct falls outside the statute as drafted. It rectifies that gap by treating such conduct as a regulatory violation, the category where *Cox* locates strict liability. That drafting choice disposes of the scienter problem that would otherwise sink an algorithmic claim.

It does nothing for the loss problem, and that is what makes Theory One hard. A per se violation still leaves the private plaintiff at the *Robey* wall. A shopper charged a personalized price has, on the defense view, bought conforming goods at a price she accepted. An objection that she would have paid less without the profiling is the same reference-price complaint *Robey* rejected. A private claim therefore lives or dies on a single question: is a personalized markup an objective, measurable disparity, or merely a higher price the consumer agreed to pay for goods she wanted?

When AI is used not to price but to deceive, through fabricated scarcity timers, synthetic customer reviews, deepfaked endorsements, AI-generated fictitious reference prices, and the *broader family of manipulative "dark patterns," the conduct fits the CFA's existing categories without strain.*

Dugan is where plaintiffs will look for an answer, but whether it supplies one is genuinely unsettled, because *Robey* and *Dugan* measure different disparities. *Robey*'s measurable disparity is the gap between the product a consumer expected and the product received, a value-based, benefit-of-the-bargain concept. *Dugan*'s differential, by contrast, arose in a class-certification ruling about how loss may be proved, not a holding that a cross-consumer price gap is itself a cognizable loss. The Court there rejected a market-wide price-inflation theory, in which an expert constructs a hypothetical fair-price benchmark. That approach, it held, is the equivalent of fraud on the market, a theory New Jersey has never extended to CFA claims.27 An expert's opinion about a fair price is no substitute for proof of an actual claimant's loss and causation.28 The same opinion, however, approved a different theory. Where the seller's own records show that customers paid different prices for the same item, those records can support findings of ascertainable loss and causation, and can carry a class through certification.29 The Court applied that logic to the companion *Bozzi claim*, holding that a class narrowed to customers charged two different prices for the same beer during a single visit could go forward, because each claimant's loss is documented on a receipt in the seller's own records.30

Personalized pricing has the same documentary quality. The harm the Legislature is pursuing is the practice of charging individual shoppers different prices for the same item at the same time, the precise disparity the bills describe.31 It is recorded in the algorithm's own logs, not dependent on an expert's reconstruction. That documentary quality is what separates a workable personalized-pricing claim from the fraud-on-the-market theory *Dugan* forbids. A plaintiff who can show from the defendant's records that she paid more than a comparable shopper paid for the same good at the same moment has her proof in the one form the Court has been willing to credit. *Dugan*'s successful theory works best where comparable shoppers and the transactional period are easy questions. One person bought two beers during one visit. An algorithm segmenting consumers by computed willingness to pay may not leave such a clean record. Whether two shoppers are truly comparable or whether two prices are truly contemporaneous can be disputed. Where *Dugan* opens the door, legislation could explicitly allow victims of personalized pricing to enter.

All of this leads back to the enforcer. Because the loss requirement constrains only private suits, a statute enforced by the Division of Consumer Affairs avoids the *Robey* problem, while a statute that creates a private right of action runs straight into it. Each time the Legislature selects an enforcement mechanism, it makes a doctrinal choice it may not have intended. Part IV returns to the point.

C. Theory Two: AI as an amplifier of ordinary deception the statute already reaches

The second problem runs the other way. When AI is used not to price but to deceive, through fabricated scarcity timers, synthetic customer reviews, deepfaked endorsements, AI-generated fictitious reference prices, and the broader family of manipulative "dark patterns," the conduct fits the CFA's existing categories without strain. These are affirmative misrepresentations and unconscionable commercial practices under Section 56:8-2, the core of the statute, and they require no proof of intent.32 An AI-fabricated former price already violates the fictitious-pricing regulation,33 and a false statement about the size of a price reduction already violates the regulation that bars misrepresenting the amount of a reduction.34

AI changes the scale and the polish of this deception, and it makes detection harder, but it does not change the legal character of the conduct. A merchant who uses a generative model to manufacture reviews needs no new statute to be liable. Such a model is only the instrument of a misrepresentation the CFA has reached for decades. The one obstacle to a private claim is the obstacle common to every CFA case, ascertainable loss. And on that point *Robey* cuts against the plaintiff even here, because it holds that deception by itself, in the form of a fictitious reference price, does not establish a loss when the consumer received conforming goods at the agreed price.35 The deceived buyer must still identify a measurable disparity.

D. Why the distinction matters

The two theories occupy very different doctrinal worlds. Theory One involves conduct the statute cannot reach unaided, conduct the Legislature is now addressing through a strict-liability per se rule, and conduct that still faces a real ascertainable-loss barrier in private litigation, one that *Dugan* narrows and that falls away only when the Attorney General is the enforcer. Theory Two involves conduct the statute already reaches, limited by the same loss requirement but needing no new law.

For the practitioner, the lesson is that the contested questions will not concern whether AI-enabled conduct is fraudulent in the abstract. They will concern loss and enforcer: whether a documented pricing differential is a cognizable injury after *Robey* and *Dugan,* and whether the Legislature has routed enforcement to a forum where the loss requirement even applies. Part III turns next to the criminal track; Part IV takes up both questions.

III. The Criminal Track and Its Gaps

Chapter 40 rewards a close read, because its architecture explains both its reach and its blind spots. The definition is broad. Deceptive audio or visual media covers video, sound recordings, electronic images, photographs, technological representations of speech or conduct derived from them, and even forgeries of documents, so long as a reasonable person would take the work to realistically depict speech, conduct, or writing that never occurred and the production depended on technical means rather than ordinary impersonation.36 The offenses are purpose-built in the literal sense. Creating such a work for the purpose of attempting or furthering any crime or offense is a crime of the third degree, as is soliciting, disclosing, or using one for that purpose, and a knowing or reckless disclosure of a work created in violation of the statute is a crime of the fourth degree.37 Violations carry an enhanced fine of up to $30,000, convictions do not merge with the underlying offense, and consecutive sentencing is mandatory.38

The Legislature wanted the punishment cumulative and said so in the findings.[39]

The civil remedy deserves more attention than it has received. The action belongs to the victim, and the statute defines victim generously, reaching not just the person depicted but anyone who suffers personal, physical, or psychological injury or a loss of or injury to property as a result of the violation.[40] A criminal conviction is not a prerequisite. The Superior Court may award actual damages with a liquidated floor of $1,000 for each knowing or reckless violation, punitive damages on proof of willful disregard, attorney's fees, and equitable relief.[41] Further, the action is cumulative with defamation, false light, and misappropriation claims rather than a substitute for them.[42] A business defrauded by a cloned voice can, at least on paper, plead its way into the section; theft and fraud offenses sit on the statute’s own illustrative list of predicates.43

The civil remedy deserves more attention than it has received. The action belongs to the victim, and the statute defines victim generously, reaching not just the person depicted but anyone who *suffers personal, physical, or psychological injury or a loss of or injury to property as a result of the violation.*

The limits appear in practice rather than on the surface. Both the crimes and the civil liability attach only to a natural person, so the defendant is the individual operator, who in a commercial fraud is routinely anonymous, out of state, or judgment-proof. The exemptions then place the parties actually worth suing beyond reach.

Interactive computer service providers, cloud providers, and commercial developers and providers of artificial intelligence technology are outside the act, and broadcasters and advertising channels are carved out in most configurations.44 The plaintiff must still prove conduct that would violate the criminal provisions, purpose element included, and nothing in the act requires anyone to take the forgery down. What the section delivers, in the commercial setting, is a damages claim against the person least likely to pay it.

The legislative pipeline behind chapter 40 is meanwhile consolidating around intimate imagery, understandably given the harms that pushed the bill to the governor's desk.45 S. 3303 would fold AI-generated images into the voyeurism and nonconsensual-disclosure crimes.46 The federal TAKE IT DOWN Act criminalizes the nonconsensual pub lication of intimate visual depictions, including digital forgeries. Its notice-and-removal mechanism, mandatory for covered platforms since May 19, 2026, and enforced by the Federal Trade Commission, gives victims of intimate deepfakes the one thing chapter 40 does not: a way to get the content removed.47 That removal right stops at intimate depictions. A company confronting a fabricated video of its own chief financial officer circulating among customers has no takedown mechanism under any of these laws, a criminal remedy that depends on a prosecutor's interest, a civil claim aimed at an anonymous natural person, and, for the reasons Part II explains, no route through the Consumer Fraud Act, because a duped wire transfer is not a consumer transaction.

There is also an evidence problem, and it will arrive ahead of any legislative fix. Every deepfake dispute becomes, sooner or later, an authentication dispute under N.J.R.E. 901, which asks only for evidence sufficient to support a finding that the item is what its proponent claims.48 New Jersey courts have met each new medium by applying that conventional standard rather than inventing a heightened one. The Appellate Division took exactly that approach to social media in *State v. Hannah,* holding the existing standards adequate and authenticating a tweet through its content, its nature as a reply, and details only a participant would know.49 To the objection that a tweet is easily forged, the court answered that so is a letter.50 Synthetic media is the first technology built to defeat that answer, because the forgery is engineered to carry the very indicia the rule looks for. The proponent of genuine evidence now faces manufactured doubt, the objection that authentic media has been fabricated, a tactic commentators have named “the liar’s dividend.”51 The opponent of fabricated evidence must expose a fake designed to pass. No published New Jersey decision has yet confronted an alleged deepfake, and until one does, the practical answers are the familiar ones performed more carefully: chain of custody, metadata and provenance discovery, testimony from participants with personal knowledge, and, where the stakes justify it, forensic analysis presented at a Rule 104 hearing. Authentication fights that used to take a sentence should be budgeted to take an expert.

The criminal track, in sum, has the right instincts and a narrowing field of view: severe, cumulative punishment for deepfakes tied to crime, a civil action built to compensate the depicted and the injured, and nothing designed for the synthetic forgery as an instrument of commercial fraud. Part IV turns to what the Legislature should do about it, on this track and the other one.

IV. Where the Law Should Go

New Jersey has been legislating one headline at a time. Deepfakes produced a criminal statute in 2025. Grocery pricing produced the Fair Price Protection Act, now on the governor's desk.52 Rent-setting algorithms have a bill of their own,53 and pornographic deepfakes another.54 Each measure responds to a genuine harm. Each was also drafted as though the case law described in Part II did not exist, and that case law decides who can sue and for what. Four choices, each aimed at a specific holding rather than a general mood, would turn the accumulating measures into a framework.

A. Define the ascertainable loss, or private enforcement is an illusion

The hardest holding to legislate around is *Robey.* A shopper who pays a personalized price has bought conforming goods at a price she accepted, and on that reasoning she has suffered no ascertainable loss however unlawful the pricing practice may be.55 A statute that declares surveillance pricing a per se unlawful practice therefore accomplishes less than it appears to accomplish. The private plaintiff clears the unlawful-practice element and, absent the kind of clean records present in *Dugan*, stalls at the loss element. If the Legislature wants consumers to enforce these prohibitions themselves, it has to say what the loss is. The fix is a single definition: the difference between the price the consumer paid and the lowest price the seller contemporaneously charged or offered a similarly situated consumer for the same item is deemed an ascertainable loss.

That definition does not fight the Supreme Court. It follows the Court's own map. *Dugan* allowed a claim built on the seller's records showing that customers paid different prices for the same item to proceed, and it let those records carry loss, causation, and class certification.56 What *Dugan* forbade was the expert-built benchmark, a hypothetical fair price constructed for litigation.57 A statutory differential measured against the seller's own contemporaneous pricing takes what *Dugan* only pointed toward and writes it into law, removing the uncertainty a private plaintiff would otherwise face. The proof sits in the algorithm's logs, and a records-retention requirement obligating covered sellers to preserve their pricing data would make the theory litigable in practice rather than in principle only. Nothing about the definition invites speculation. It substitutes the defendant's data for the expert the Court excluded.

B. Choose the enforcer deliberately

The loss requirement is a prerequisite for a private cause of action and does not constrain the Attorney General,58 so the choice of enforcer is not housekeeping. It determines whether *Robey* applies at all. The Fair Price Protection Act supplements the Consumer Fraud Act itself,59 which leaves the question live. If the final law is silent, courts will have to decide whether the treble damages and fee-shifting of Section 56:8-19 attach to the new prohibition.60 The committee substitute that advanced in March paired a fixed civil penalty with an enforcement action by the Attorney General, which suggests the drafters leaned toward public enforcement without quite saying so.61

Either design is defensible. A regime run by the Attorney General sidesteps *Robey,* centralizes technical expertise, and echoes the statute's original architecture, since the 1960 Act gave the Attorney General exclusive authority and the private right arrived by amendment in 1971.62 A private right multiplies enforcement and compensates the shopper who was actually overcharged, but after *Robey* it works only if it is paired with the loss definition above. What is not defensible is silence, which converts a policy choice into a decade of motion practice. If the choice is public enforcement, it should be funded like one; the pending bill that would stand up a Deepfake Technology Unit shows the Legislature knows how to build capacity when it intends an agency to act.63

C. Close the commercial deepfake gap

The 2025 deepfake law is organized around a criminal predicate. It reaches deceptive audio or visual media created or used for the purpose of furthering a crime, carries third-degree exposure with fines up to $30,000, and gives victims a civil action against the natural person who committed the violation.64 The measures behind it are consolidating the criminal track around intimate imagery,65 and the federal TAKE IT

DOWN Act does the same at the platform level, with a removal mechanism confined to intimate depictions.66 None of this reaches the deepfake deployed for commercial theft. The cloned voice of a managing partner authorizing a wire transfer, the synthetic invoice from a vendor who never sent one, the fabricated video of a counterparty approving terms: these are the fact patterns already reaching commercial litigators, and the coverage they find is thinner than it looks. The deepfake statute's civil action requires the plaintiff to establish conduct that would violate the criminal provisions, purpose element included; it runs only against natural persons, leaving the anonymous operator as the sole defendant while the exemptions shelter the platforms, hosts, and toolmakers; and it awards damages without any mechanism for getting the forgery taken down. The Consumer Fraud Act cannot absorb the claim either, because its prohibitions run to deception in connection with the sale or advertisement of merchandise or real estate,67 and none of these frauds occurs inside a consumer transaction. The victims are often businesses, the losses are documented to the dollar, and the remedy on the books was built around a different paradigm.

The repair is a freestanding civil cause of action for pecuniary loss caused by the knowing creation or use of synthetic media to deceive, one that reaches any person rather than only natural persons and that carries no consumer-transaction predicate, no intimate-imagery predicate, and no requirement that the plaintiff first establish a criminal purpose. Actual damages, fee-shifting, and injunctive relief would carry the CFA's remedial philosophy into the space without importing its transactional limits. The criminal statute's exemptions for criticism, comment, satire, parody, news reporting, teaching, scholarship, and research can carry over intact, which answers the First Amendment objection the same way the Legislature already answered it.68

D. Consolidate before the patchwork hardens

Count the instruments. A criminal deepfake statute. A grocery pricing act supplementing the CFA. A rental-algorithm bill on its own track.69 A voyeurism amendment for pornographic deepfakes. A federal platform overlay. Five measures in roughly two years, with different intent standards, different enforcers, and different remedies, all aimed at one phenomenon, machine-generated deception. The better course is a single chapter that defines synthetic media and algorithmic pricing once, enumerates the per se practices, assigns scienter deliberately, with strict liability in the pricing lane where *Cox* already places regulatory violations70 and a knowledge standard for synthetic-media deception where speech concerns demand it, writes the loss definition into the text, and makes the enforcement election expressly. That is not a proposal for an omnibus artificial intelligence code. It is a proposal to consolidate the deception provisions New Jersey has already decided to write before their inconsistencies become precedent.

The courts have marked the walls with unusual clarity. *Robey* says what counts as a loss, *Dugan* says how it may be proved, and *Weinberg* says who must prove it. A Legislature that drafts against those holdings, rather than around them, would give practitioners on both sides of these cases something the current approach cannot: a predictable answer to whether AI-enabled conduct is actionable in New Jersey, by whom, and for what.

Endnotes

1. P.L. 2025, c. 40 (codified at N.J.S.A. 2C:21-17.7 *et seq.*) (approved Apr. 2, 2025).

2. N.J.S.A. 2C:21-17.8(f).

3. N.J.S.A. 2C:21-17.8(g).

4. S. 3303, 2026-2027 Leg. Sess. (N.J.) (pending as of July 15, 2026).

5. A. 3058, 2026-2027 Leg. Sess. (N.J.) (pending as of July 15, 2026).

6.TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55 (2025).

7.A. 4085/A. 4523 (Assembly Committee Substitute), 2026-2027 Leg. Sess. (N.J.) (Fair Price Protection Act) (passed both Houses June 30, 2026; awaiting action by the Governor as of July 15, 2026) (supplementing N.J.S.A. 56:8-1 *et seq.*).

8. Press Release, Consumer Reports, Consumer Reports Statement on New Jersey

Fair Price Protection Act to Ban Personalized Pricing in Grocery Sales (June 30, 2026); *see also New Jersey Surveillance Pricing Ban Heads to Governor,* NJBIZ (July 7, 2026).

9. S.3952, 2026-2027 Leg. Sess. (N.J.) (as introduced; pending as of July 15, 2026).

10. A.3989, 2026-2027 Leg. Sess. (N.J.) (pending as of July 15, 2026).

11.N.J.S.A.56:8-19.

12. *Cox v.Sears Roebuck & Co.,* 138 N.J.2, 17 (1994).

13. *Id.*at 17-18.

14. *Id.*at 18.

15. *Id.*at 18-19.

16. *Lee v.Carter-Reed Co.,* 203 N.J.496, 521 (2010).

17. *Thiedemann v.Mercedes-Benz USA, LLC*, 183 N.J.234, 248 (2005).

18. *Id.* at 248-49.

19. *See Weinberg v.Sprint Corp.*, 173 N.J.233, 237 (2002); *Thiedemann*, 183 N.J.at 246, 249-51.

20. *Robey v.SPARC Grp., LLC,* 256 N.J.541, 548-49 (2024).

21. *Id.* at 549.

22. N.J.S.A.56:8-2.5.

23. N.J.S.A.56:8-21 et seq.; N.J.A.C.13:45A-14.1 et seq.

24*. Dugan v.TGI Fridays, Inc.*, 231 N.J.24, 34 (2017).

25. S.3952, supra note 9.

26.Fair Price Protection Act, *supra* note 7.

27. *Dugan,* 231 N.J.at 34.

28. *Id.*

29. *Id.*at 34-35.

30. *Id.*at 41-42, 64-66 (sustaining certification of the class as narrowed to the price-shifting claim, while reserving whether the practice violates the CFA).

31.Fair Price Protection Act, *supra* note 7.

32. *Cox,* 138 N.J.at 17-18.

33. N.J.A.C.13:45A-9.6.

34. N.J.A.C.13:45A-9.2(a)(9); *see Furst v.Einstein Moomjy, Inc.,* 182 N.J.1 (2004).

35. *Robey,* 256 N.J.at 548-49.

36. P.L.2025, c.40, *supra* note 1. The operative definitions and offenses appear at N.J.S.A.2C:21-17.8.

37. N.J.S.A.2C:21-17.8(b), (c).

38. N.J.S.A.2C:21-17.8(d), (e).

39. N.J.S.A.2C:21-17.7.

40. N.J.S.A.2C:21-17.8(a).

41. N.J.S.A.2C:21-17.8(f).

42. *Id.*

43. N.J.S.A.2C:21-17.8(b)(1).

44. N.J.S.A.2C:21-17.8(g).

45. Press Release, Office of the Governor, Governor Murphy Signs Bipartisan Legislation Establishing Civil and Criminal Penalties for Deceptive AI Deepfakes (Apr. 2, 2025).

46. S.3303, *supra* note 4.

47.TAKE IT DOWN Act, *supra* note 6.

48. N.J.R.E.901; *see also* N.J.R.E.104.

49. *State v.Hannah,* 448 N.J.Super. 78 (App. Div. 2016).

50. *Id.*

51. Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 Calif. L.Rev.1753 (2019).

52. Fair Price Protection Act, *supra* note 7.

53. A.3989, *supra* note 10.

54. S.3303*, supra* note 4.

55. *Robey,* 256 N.J.at 548-49.

56.*Dugan*, 231 N.J.at 34-35.

57. *Id*.at 34.

58. See *Weinberg,* 173 N.J.at 237; *Thiedemann,* 183 N.J.at 246, 249-51.

59. Fair Price Protection Act, *supra* note 7.

60. N.J.S.A.56:8-19.

61. S.3612/S. 3717 (Senate Committee Substitute), 2026-2027 Leg. Sess. (N.J.) (as reported by the Senate Commerce Committee, Mar.16, 2026).

62. *Cox,* 138 N.J.at 14-15.

63. A.3058, *supra* note 5.

64. P.L.2025, c.40, *supra* note 1.

65.S.3303, *supra* note 4.

66. TAKE IT DOWN Act, *supra* note 6.

67. N.J.S.A.56:8-2.

68. P.L.2025, c.40, *supra* note 1.

69. A.3989, *supra* note 10.

70. *Cox,* 138 N.J.at 18-19.

ASAAD K. SIDDIQI »

ASAAD K. SIDDIQI *is a director at Trenk Isabel Siddiqi & Shahdanian P.C. in Livingston and Hackensack, where his practice includes commercial litigation, employment law, and business counseling. He serves on the Board of Trustees of the New Jersey State Bar Association, the Association of the Federal Bar of New Jersey, and the Bergen County Bar Association, and is a member of the New Jersey Lawyer editorial board, which he previously chaired.*

LUKE D. GRYGIER *is an associate at Trenk Isabel Siddiqi & Shahdanian P.C., where his practice focuses on commercial*

LUKE D. GRYGIER »

litigation, including securities, Consumer Fraud Act, and employment matters.