| | |
|---|---|
| STATE OF NEW JERSEY,<br><br>Plaintiff-Appellant,<br><br>v.<br><br>TYBEAR MILES,<br><br>Defendant-Respondent. | SUPREME COURT OF NEW JERSEY<br>DOCKET NO. 090275<br><br>Criminal Action<br><br>On Motion for Leave to Appeal from an Interlocutory Judgment of the Superior Court of New Jersey, Appellate Division.<br><br>Sat Below:<br><br>Hon. Jessica R. Mayer, P.J.A.D.<br>Hon. Patrick DeAlmeida, J.A.D. |

# BRIEF OF *AMICUS CURIAE* NEW JERSEY STATE ASSOCIATION OF CHIEFS OF POLICE

**PORZIO, BROMBERG & NEWMAN, P.C.**
100 Southgate Parkway
Morristown, NJ 07960
973-538-4006
Attorneys for Amicus Curiae New Jersey State Association of Chiefs of Police

*Of Counsel:*
Vito A. Gagliardi, Jr., Esq. (024821989)

*On the Brief:*
David L. Disler, Esq. (068112013)
Thomas J. Reilly, Esq. (245552017)

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

Page(s)

## CASES



## NEW JERSEY RULES OF EVIDENCE



## NEW JERSEY COURT RULES

## PRELIMINARY STATEMENT

Defendant seeks to expand his right to discovery beyond the express limits imposed by this Court and, until recently, by the Appellate Division. In particular, he demands access to the source code and other proprietary information of facial recognition technology ("FRT") that the State does not seek to introduce at trial and that played only a minimal role in the investigation leading to his arrest. Prior appellate case law establishes that a defendant must demonstrate a "particularized need" for such discovery, and this Court's prior witness identification case law ties that need to an intolerable risk of suggestiveness in the identification process -- a risk that is completely absent here.

This case arises in the context of a murder investigation. Police provided surveillance video of a potential suspect to a confidential informant. The informant knew the suspect by his "street name" and Instagram handle (*i.e.*, username). Based on the information provided by the informant, detectives took a picture from the Instagram account and uploaded it to an FRT module, which then returned a list of booking photographs of potential matches. The confidential informant positively identified Defendant by his booking photograph as the person he believed to be in the surveillance video. FRT would not be used again in the investigation, nor does the State plan to introduce it at

trial. With knowledge of Defendant's identify, detectives interviewed his sister and ex-girlfriend, both of whom positively identified him in the video.

Given the confidential informant's role in the investigation, the limited use of FRT as an investigative tool at an early stage in the investigation, and the confirmatory nature of the witness identifications, the attendant risk that FRT created undue suggestiveness here is non-existent. That alone should foreclose Defendant's ability to obtain discovery of the FRT source code and other proprietary information. Moreover, the State disclosed to Defendant the manner in which FRT was used, and Defendant remains free to obtain further discovery regarding the ways in which detectives used the FRT. He should not have the ability to obtain proprietary software information absent a compelling and particularized need for it, which he cannot show.

Defendant's arguments rely heavily on a single Appellate Division case: *State v. Arteaga*, 476 N.J. Super. 36 (App. Div. 2023), in which the panel held that a defendant was entitled to proprietary information regarding FRT used by a New York City police lab. The *Arteaga* panel reached its holding through vague concerns of "due process," and by relying on prior Appellate Division cases in which the court held that discovery of proprietary software information could be had to test the veracity of expert witness testimony **only** – and even then only upon a showing of a particularized need for the information. By

expanding that prior case law outside the purview of expert testimony, *Arteaga* went too far. Moreover, despite its due process concerns, *Arteaga* failed to import this Court's jurisprudence regarding suspect identification, which requires that a defendant show an intolerable risk of suggestiveness regarding the identification methodology at issue.

This Court can correct *Arteaga* here by uniting its suspect identification jurisprudence with the prior case law that *Arteaga* improperly expanded. This single framework would permit a defendant to access source code and other proprietary FRT information only upon a showing of a particularized need, evidenced by an intolerable risk of suggestiveness. A defendant would not be able to make that showing where, as here, the FRT is not introduced at trial and plays only a supporting role in the investigation. Such a framework would strike the appropriate balance by providing defendants with the due process to which they are entitled, while also preventing them from weaponizing discovery and overburdening law enforcement agencies with exploratory discovery demands. Indeed, many of the state's smaller law enforcement agencies may lack the resources -- and indeed even the prerogative -- to produce extensive discovery of third-party proprietary information. A more limited and nuanced approach, in accordance with this Court's prior jurisprudence, is therefore the appropriate measure to strike the proper balance.

## PROCEDURAL HISTORY AND STATEMENT OF FACTS

*Amicus curiae* New Jersey State Association of Chiefs of Police ("NJSACOP") relies upon the procedural history and statement of facts set forth in the State's brief.

## LEGAL ARGUMENT

### THE COURT SHOULD BUILD UPON ITS PRIOR CRIMINAL DISCOVERY AND IDENTIFICATION CASE LAW TO CREATE A FRAMEWORK THAT PERMITS DISCOVERY OF FRT SOFTWARE AND SOURCE CODE ONLY WHERE A CRIMINAL DEFENDANT DEMONSTRATES A PARTICULARIZED NEED FOR IT.

No party disputes that criminal defendants are entitled to broad pretrial discovery sufficient to allow the presentation a complete defense. Pressler & Verniero, *Current N.J. Court Rules*, cmt. 3.2 on *R.* 3:13-3 (2025). Those broad discovery rights do not permit criminal defendants to obtain any information they wish, however. Rather, courts limit discovery in criminal cases to information that is both "probative" and "material[]," meaning the information is "really in issue in the case." *State v. Buckley*, 216 N.J. 249, 261 (2013). Not all police investigatory work or processes meet this materiality standard. Indeed, this Court expressly has recognized that certain information upon which the police rely in their investigatory work is not subject to disclosure if it is not otherwise introduced into evidence. *See State v. Milligan*, 71 N.J. 373, 383-84 (1976) (discussing "informer's privilege" and denying request to discover

identity of confidential informant); *N.J.R.E.* 516 (codifying the informer's privilege). As the United States Supreme Court has noted, there is "no constitutional requirement that the prosecution make a complete and detailed accounting to the defense of all police investigatory work on a case." *Moore v. Illinois*, 408 U.S. 786, 795 (1972).

Defendant here seeks to obtain source code and other software proprietary information regarding the FRT detectives used, even though the State does not plan to introduce it into evidence at trial, through expert testimony or otherwise. Defendant's arguments are at odds with the prior case law regarding both discovery and witness identifications. The entirety of the Appellate Division's prior case law -- save for a single case, *State v. Arteaga*, discussed in greater detail below -- holds that a criminal defendant is not entitled to discover proprietary software information unless the State plans to introduce it at trial, and, even then, only where the Defendant demonstrates a compelling need. Relatedly, this Court's jurisprudence regarding eyewitness identifications espouses the principle that a defendant bears the burden to show that an identification procedure creates an intolerable risk of misidentification.

Taken together, these principles yield a common sense result here: a criminal defendant should be permitted access to FRT source code and other proprietary information only upon showing a compelling or particularized need

for the information because the information creates an intolerable risk of misidentification or is unduly suggestive. Such a standard will protect the due process rights of criminal defendants based on standards and principles applied by this Court in the past, while also protecting law enforcement agencies from burdensome, onerous, and searching discovery demands for proprietary information that the law enforcement agency may not own, possess, or easily extract and produce.

### A. Appellate Case Law Prior To *Arteaga* Permitted Discovery Of Proprietary Source Code And Related Information Only Where The State Sought To Use The Software At Trial, and Only Then Upon A Showing Of Particularized Need.

Several years ago, a tandem of Appellate Division cases created a framework for assessing a criminal defendant's access to software, source code, and other technological proprietary information. Those cases permitted the defendant to obtain the information only if the State chooses to rely upon it at trial. For example, in *State v. Pickett,* the State sought to introduce expert testimony supported by a "complex probabilistic genotyping software program to testify that [the defendant's] DNA was present" at a murder scene. 466 N.J. Super. 270, 277 (App. Div. 2021). The defendant sought trade secret information related to the software, including its source code and other similar data. *Id.*

The Appellate Division expressly tied the defendant's right to obtain discovery of the requested proprietary information to the State's introduction of the software into evidence. The panel held that a "defendant is entitled to access . . . the software's source code and supporting software development and related documentation" "**[i]f the State chooses to utilize an expert who relies on [the] software to render DNA testimony**." *Id.* at 279, 306-07. Even then, a defendant must show a "particularized need for such discovery." *Id.* To show a particularized need, a criminal defendant must show: (1) a "rational basis" to order disclosure based on the "proffered expert testimony"; (2) specificity of the information sought; (3) means of assuring protection of the intellectual property sought; and (4) other relevant factors unique to the facts of the case. *Id.* In reaching its holding that the defendant was entitled to the discovery at issue, the panel explained that the defendant's right to the information was tied to his right to test the veracity and reliability of the expert testimony at issue. *See id.* at 305-06 ("Allowing independent access to the requested information, **for the sole purpose of addressing whether the technology underlying the expert testimony is reliable** -- specifically, whether the source code for that technology is properly implementing the program's design specifications -- is obvious."). *See also id.* at 301 (noting need to test expert testimony because

"there is substantial danger that juries will accord excessive weight to testimony that might otherwise be unreliable").

The *Pickett* court based its decision on an Appellate Division case decided one year prior, *State v. Ghigliotty*, 463 N.J. Super. 355 (App. Div. 2020). In *Ghigliotty*, the Appellate Division considered whether the defendant was entitled to the disclosure of algorithms, software, and other proprietary information for a ballistics imaging device known as BULLETTRAX. *Id.* at 384-85. As was the case in *Pickett*, the State sought to introduce expert testimony in which the expert relied upon the software at issue to form an opinion. *Id.* at 360. Though the Appellate Division admitted that the software "might be needed by defendant's experts to evaluate the reliability of the new technology," the panel concluded that "there is currently nothing concrete in the record to support the [trial] court's conclusion that granting defendant" the requested discovery "is necessary in order to completely explore and test the integrity of the images it produces." *Id.* at 384. The panel therefore reversed the trial court's order granting defendant access to the requested discovery, explaining that a "defendant is required to make a more definitive showing of his need for th[e] material to provide the [judge] with a rational basis to order the State to attempt to produce" the proprietary algorithms. *Id.* at 384-85.

Taken together, *Pickett* and *Ghigliotty* permit a criminal defendant to obtain discovery of proprietary software information "for the sole purpose" of testing the reliability of expert testimony, and only then upon a showing of a "particularized need" for the discovery at issue. There is no dispute that Defendant here could not meet this high bar because the State here does not seek to introduce FRT evidence through expert testimony or otherwise, and because Defendant has not attempted to, and cannot, show a particularized need for the FRT information he requests.

### B. The Appellate Division's *Arteaga* Decision Is An Unwarranted Extension of *Pickett* And *Ghigliotti* That Ignores The Limitations Inherent In Their Holdings, As Well As Broader Principles Espoused By This Court Regarding Criminal Discovery.

The Appellate Division misapplied both *Pickett* and *Ghigliotti* in its *Arteaga* decision, extending both cases beyond the express limitations set forth in their holdings. *Arteaga* concerned an armed robbery of a cell phone store carried out in November 2019. 476 N.J. Super. at 42. A store manager reviewed surveillance footage of the robbery and thought she recognized the perpetrator. *Id.* Detectives retrieved various sources of surveillance footage showing the suspect both inside and outside the store. *Id.* They then sent the surveillance footage to the Facial Identification Section of the New York Police Department Real Time Crime Center. *Id.* at 43. The Center captured a still image from the

footage, compared it against the Center's databases using FRT, and offered the defendant as a potential match. *Id.* The New Jersey detectives assigned to the case then created two different photo arrays, comprised of five filler photos and the photo Center provided of the defendant from its database. *Id.* The detectives then provided the arrays to both the store manager, who reviewed the video footage, and a store clerk, who was present at the scene, in separate videorecorded interviews. *Id.* Both witnesses independently identified the defendant's photo as that of the perpetrator. *Id.*

During discovery, the defendant's counsel sought discovery regarding the FRT tools police used to identify the defendant, including the FRT's name and manufacturer, the algorithm on which it relied, its source code, error rates, performance tests, and various other forms of proprietary information. *Id.* at 43-44. After the defendant filed a motion to compel the production of the requested information, the trial court issued a written opinion in which it held that "the State had no obligation to produce the discovery because the FRT was not within its care, custody, or control." *Id.* at 50. Defendant then moved for leave to appeal, which the Appellate Division granted. *Id.*

On appeal, the Appellate Division relied on both *Pickett* and *Ghigliotty* to hold that the defendant was entitled to the discovery he sought. As to *Ghigliotty*,

the panel noted that "a *Frye*[1] hearing was necessary" in that case because "although the expert used a traditional method to analyze the bullet, the untested, newer technology caused him to change his conclusion and 'clearly aided and influenced the course of his investigation and informed his ultimate opinion.'" *Id.* at 55. The *Arteaga* Court did not discuss or acknowledge that, though the *Ghigliotty* panel required a *Frye* hearing to determine the software's reliability because the State's experts planned to rely on it, the panel did not permit the defendant to obtain discovery regarding the software source code absent a particularized showing of need.

Similarly, the *Arteaga* Court referenced *Pickett*, but did not appreciate that *Pickett's* holding permitted the defendant independent access to the requested information "for the **sole purpose** of addressing whether the technology underlying the expert testimony is reliable." *Pickett*, 466 N.J. Super. at 305-06. Instead, the *Arteaga* panel admitted that it was "keenly aware the cases . . . discussed involved instances concerning *Frye* hearings and potential expert testimony," but believed that "the facts of this case convince [it] defendant will be deprived of due process if he does not have access to the raw materials integral to the building of an effective defense," including the ability "to

[1] This Court has since departed from the *Frye* standard, and has imported to criminal cases the factors for expert witness reliability set forth in *In re Accutane Litig.*, 234 N.J. 340 (2018). *See State v. Olenowski*, 253 N.J. 133 (2023).

impeach the witnesses' identification, challenge the State's investigation, create reasonable doubt, and demonstrate third-party guilt." *Arteaga*, 476 N.J. Super. at 36, 57.

*Arteaga's* holding strays too far from the prior appellate case law and from this Court's pronouncements. It should be either overturned or, at most, limited to its particular facts. Most importantly, *Arteaga* did not give sufficient consideration to *Pickett's* instruction that the discovery of source code and other proprietary information should be accessible **only** for the purpose of testing the veracity and reliability of expert testimony. The *Arteaga* Court rested its holding on due process concerns, but did not explain how the use of FRT implicated the defendant's due process rights in a case where the State did not intend to introduce it at trial, and where two witnesses independently picked the defendant's photograph out of an array without any assistance or enhancement from FRT.

Most critically, the *Arteaga* panel did not appreciate the distinction between FRT's use as a basis for expert testimony, and FRT's use as an investigative tool which leads law enforcement to a particular suspect, but which is not otherwise used in the witness identification process and will not be introduced at trial. By failing to scrutinize that distinction, the panel did not explain the "particularized need" that would have compelled disclosure of the

source code and other information in a case where the FRT would not be introduced at trial. Rather, the panel retreated to generalized "due process" concerns.

Even where witness identifications raise due process concerns, this Court has held that a defendant must still show a sufficient risk of misidentification, *i.e.*, a particularized need, to challenge evidence in matters regarding witness identification. *See State v. Henderson*, 208 N.J. 208, 245 (2011). Had the Appellate Division taken the step to link the prior FRT case law with this Court's witness identification jurisprudence, it would have created a more fulsome FRT discovery framework, and would have been led inescapably to the conclusion that the defendant was not entitled to the discovery he sought because he could not show a particularized need for it. Those principles should guide the Court's decision here and lead it to distinguish *Arteaga*.

### C. This Court's Witness Identification Jurisprudence Requires The Defendant To Bear The Burden To Show An Unacceptable "Risk Of Misidentification," And The Court Should Import That Standard Here As The "Particularized Need" Necessary To Warrant Discovery Of Proprietary Information.

In prior cases concerning witness identification and the risk of misidentification generally, this Court has articulated a standard by which the defendant bears the burden to show that the State seeks to introduce identification evidence bearing an intolerably high "risk of misidentification."

*Henderson*, 208 N.J. at 245 (2011) (addressing risks of misidentification). *See also State v. Hannah*, 248 N.J. 148, 181 (2021) (noting risks inherent in identification evidence that "has a rational tendency to engender a reasonable doubt" regarding the suspect's identity). The risk here that the FRT at issue created any risk of misidentification is exceedingly low. As an initial matter, the FRT served no role in the identification process other than facilitating the production of an untouched photograph of a potential suspect. Detectives used the FRT through the aid of a confidential informant who believed he knew the suspect. Officers then interviewed Defendant's sister and ex-girlfriend, who identified Defendant in surveillance footage officers had obtained through the investigation. Defendant's sister and ex-girlfriend both identified defendant, and FRT played no role in assisting them. Such confirmatory witness identifications, where the identifying persons are closely familiar with the suspect, are "not considered suggestive," and thus do not trigger probing into the possibility of suggestiveness otherwise required under *Henderson*. *See State v. Pressley*, 232 N.J. 587, 592 (2018); *Henderson*, 208 N.J. at 288. FRT's ability here to leave any indelible mark of impermissible suggestiveness on the investigation, much less the identifications, is slim or non-existent.

Indeed, the witnesses here likely had no knowledge that FRT played any role in the investigation process. The State plans to rely on those witness

identifications at trial. The FRT software itself will not be relied upon or introduced at trial. Even so, the State disclosed to Defendant the manner in which it used FRT software to obtain Defendant's photo. Defendant remains free to probe the ways in which detectives used FRT to obtain his photograph. It is not as though Defendant has been shut out of probing the process completely. He has provided no sufficiently compelling reason or evidence of suggestiveness to go deeper and obtain discovery of the FRT's source code and other proprietary software information.

In essence, the State's use of FRT here is akin to a confidential informant. In fact, as noted above, investigators used FRT here in conjunction with information from a confidential informant. The informant here did not know Defendant's name, but knew his Instagram "handle," and investigators used FRT to compare Defendant's Instagram pictures to booking photographs. Both this Court and the Rules of Evidence recognize an "informer's privilege." *State v. Milligan*, 71 N.J. 373, 383-84 (1976); *N.J.R.E.* 516. In *Milligan*, this Court explained that the informer's privilege is necessary to prevent a criminal defendant from obtaining police investigation tools; if the privilege did not provide the protection, defendants would "routinely request disclosure," in the hope that it may "gain dismissal" if "the State declines to reveal its source of information." *Id.* at 393. Accordingly, a defendant's request for information

concerning a confidential informant cannot be a "frivolous demand for information on unsubstantiated allegations of need," but rather must be based on a "strong showing of need." *Id.* at 387, 393.

The Appellate Division failed to import or consider these various principles in *Arteaga*, even though *Henderson* and its progeny bear directly on witness identification, and the informer's privilege recognizes that certain investigation tools should be insulated from discovery absent a compelling showing of need. Taken together, these principles require that a defendant make some showing of need -- such as by sufficient evidence of suggestiveness in the identification process -- before the defendant can obtain access to the investigation tool or methodology at issue.

### D. Discovery Of FRT Software, Source Code, And Other Such Proprietary Information Should Be Rare, And Subject To A Framework Under Which A Defendant Must Make A Sufficient Showing Of Need, Evidenced By An Intolerable Risk Of Suggestiveness.

Uniting these various related and relevant principles yields a common sense framework for the discovery of FRT software and proprietary information in cases where the State uses FRT only as an investigatory tool and does not plan to rely on FRT evidence at trial. In such cases, a defendant should not be entitled to access underlying software and proprietary information of FRT unless the defendant can show a "particularized need" for the information, which may

be demonstrated by showing that the FRT at issue bears a sufficiently high "risk of misidentification." *See Henderson*, 208 N.J. at 245 (holding that defendant bears burden to show risk of misidentification); *Milligan*, 71 N.J. at 387, 390, 393 (noting that defendant must make a "special showing" to bypass informer's privilege); *Pickett*, 466 N.J. Super. at 279, 306-07 (holding that defendant must show a "particularized need" for discovery of FRT source code and other similar information). That would not be the case where, as here, FRT "plays only a marginal role, such as providing information or 'tips' to the police or participating in the preliminary stage of a criminal investigation." *Milligan*, 71 N.J. at 387.

FRT source code and software therefore should be discoverable only in the rare instance where it is central to the State's case or integral to the identification process, such as where it produces a random or uncorroborated lead to a particular suspect, where it enhances a suspect's photograph for identification purposes, or where it is relied upon by an expert witness. It would not be the case where, as here, it is used in conjunction with a confidential informant to obtain an untouched photograph that is then shown in a confirmatory identification. *See Pressley*, 232 N.J. 587, 592 (2018) (noting that confirmatory identifications are not suggestive in nature).

In most cases, the FRT's actual design and inner workings are unlikely to lead to probative evidence sufficient to meet a particularized need of the defendant. Of course, a defendant would remain free to obtain discovery and to adduce testimony at trial regarding how the FRT was used. For example, whether the FRT was used in conjunction with an informant, as it was here, whether it produced an independent lead based on enhancement of video footage, whether it produced other "matches" aside from the defendant, and other similar information. A defendant can obtain this information without discovery of the FRT's software, source code, and other proprietary information. Certainly, a defendant also would be entitled to obtain discovery of the FRT's proprietary information to the extent the State plans to use the FRT for evidence introduced at trial, but it should be the rare case where a defendant is entitled to such information if the FRT is used only as an investigative tool.

In addition to conforming with prior case law regarding a criminal defendant's access to discovery, the framework described herein will protect law enforcement agencies from overly burdensome, if not outright disruptive, discovery demands for proprietary software that the agencies do not own or control. Typically, "[t]he State is not obliged to produce testing-related documents unless they 'are within the possession, custody or control of the prosecutor.'" *State v. Washington*, 453 N.J. Super. 164, 180 (App. Div. 2018),

but a court may nonetheless require the State to do so by exercising "its inherent power to order discovery outside the court rule." *State v. Kane*, 449 N.J. Super. 119, 133 (App. Div. 2017). The defendant rightfully bears the burden in such cases, given that a law enforcement agency may face significant challenges in producing extensive discovery of sensitive software it does not own.

In particular, granting a defendant broad and unfettered access to sensitive software, even when that software is not introduced at trial, will incentivize defendants to weaponize discovery and send blanket requests for extensive, burdensome, and proprietary information to law enforcement agencies throughout the state, both big and small, which must then assume the burden of producing the information. Our concern is that these law enforcement agencies may only be able to do so with the consent and participation of third-party software developers who do not wish to produce their proprietary source codes, who may wish to oversee the process or produce the information themselves, or who may no longer want to risk providing the software to law enforcement agencies given the chance that it may be subject to production. *See Milligan*, 71 N.J. at 392-93 (noting the risks in permitting criminal defendants to engage in broad discovery of law enforcement investigative resources). The result would be a morass of discovery demands served on overburdened law enforcement agencies, which may lack the resources or expertise to produce the information,

and which may be exposed to various forms of liability for failing to timely and accurately produce complex information they do not own or even oversee. It should be the very rare case where a court imposes this burden on a law enforcement agency.

Moreover, permitting such discovery would contravene this Court's instruction that a criminal defendant should not be permitted to engage in "an unfocused, haphazard search for evidence." *State v. D.R.H.*, 127 N.J. 249, 256 (1992). *See R.* 3:11(d) (requiring law enforcement agencies to "obtain and preserve" the "details" of an "out-of-court investigation procedure" only if it is "feasible" to do so). NJSACOP seeks nothing more here than what this Court already has held in previous and related cases.

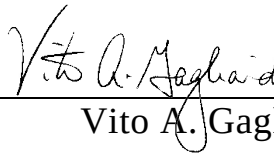
By tying the Appellate Division's holdings in *Pickett* and *Ghigliotty* to the standards for witnss identification set forth by this Court in *Henderson* and its progeny, the Court can strike the appropriate balance between permitting defendants to obtain sensitive proprietary data when it is necessary to test the reliability of FRT that will create an undue risk of suggestibility, while also protecting law enforcement agencies from weaponized and haphazard discovery practices of the type this Court always has guarded against. Applying those principles here leads to an inescapable result: Defendant is not entitled to the discovery he seeks because he has not shown, and cannot show, a particularized

need for it, particularly given the exceedingly low risk of suggestibility inherent in the way FRT was used here.

## CONCLUSION

For the forgoing reasons, NJSACOP respectfully requests that the Court reverse the trial court's order compelling the State to produce the FRT discovery requested by Defendant.

**PORZIO, BROMBERG & NEWMAN, P.C.**
Attorneys for Amicus Curiae New Jersey State Association of Chiefs of Police

By: 
Vito A. Gagliardi, Jr.

Dated: August 20, 2025