Privacy, Data and Cyber Security: The Current Legal Landscape

PIETRAGALLO
PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP

MDCPA.CNF.IO

- Navigate to https://mdcpa.cnf.io and tap the session titled "Cybersecurity"

- OR just point your phone's camera at the QR code to join directly

PIETRAGALLO
PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP

Agenda

DATA PRIVACY

- PRIVACY V. SECURITY
- CURRENT STATE OF PRIVACY LAWS IN THE UNITED STATES
- STATE CONSUMER PRIVACY LAWS
- KEY RIGHTS AND OBLIGATIONS UNDER STATES LAWS
- ENFORCEMENT
- TRENDS IN PRIVACY LAWS
- DATA BREACH NOTIFICATION LAWS
- KEY TAKEAWAYS

DATA SECURITY

- ESSENTIAL CONCEPTS
- CYBER THREATS
- DATA BREACH
- LEGAL FRAMEWORK FOR CYBERSECURITY
- INDUSTRY
- GUIDANCE
- BEST PRACTICES

Data Privacy

CHRISTOPHER A. IACONO, PARTNER

PIETRAGALLO
PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP

Definition – Data Privacy Versus Data Security

- Data privacy focuses on the use and governance of personal data

- Data security focuses on protecting data from attacks and preventing exploitation of stolen data

https://law.asia/regional-data-privacy-laws/

Current State of Privacy Laws in the United States

Different Types of Privacy Laws In The U.S. Generally

- There is no all-encompassing federal law in the U.S. regulating data privacy. However, individual steps have taken steps to enact privacy-driven laws, and certain federal regulation has been passed to regulate certain industries.
- Types of privacy laws include data privacy laws, breach notification laws, and biometric privacy regulations.
- Industry-specific laws include:

FERPA

HIPAA

COPPA

GLBA

PIETRAGALLO
PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP

State Consumer Privacy Laws

Current State Consumer Privacy Laws

- Only **three** states have comprehensive consumer privacy laws
  - California – California Consumer Privacy Act (CCPA)
    - California Privacy Rights Act (CPRA)
  - Virginia – The Virginia Consumer Data Protection Act
  - Colorado – The Colorado Privacy Act

Key Rights and Obligations Under State Laws

Consumer Rights

1. Right of Access
2. Right of Rectification
3. Right of Deletion
4. Right of Restriction
5. Right of Portability
6. Right of Opt-Out
7. Right Against Automated Decision Making
8. Private Right of Action

Business Obligations

1. Opt-in requirement age
2. Notice/Transparency requirement
3. Risk Assessments
4. Prohibition of Discrimination
5. Purpose/Processing Limitation

2021 Proposed Federal Legislation

- SAFE DATA Act and Consumer Data Privacy Act

Enforcement

- Private rights of action
- Suits brought by state attorney generals
- Federal Trade Commission (FTC) Enforcement

Other Trends in Privacy Legislation

- Biometric Privacy
  - Illinois Biometric Information Privacy Act (BIPA) (IL)
  - New York City Biometric Privacy Law

Breach Notification Laws

- Breach notification laws require companies to notify individuals in the event of a breach and require significant procedural safeguards to reasonably insure against breaches and data hacks
- Key features:
  - Broad definition of “breach”
  - Definition of Personal Information covered
  - Covered entities
  - Who needs to be notified, how, and when
  - What information to include in notice
  - Notice requirements to AG or state agency
  - Penalties and rights of action (either AG or private) (CCPA 1st w/ statutory damages)

Key Takeaways

Privacy and security are now an important part of conducting business every day

Companies that fail to take action ignore compliance risk

Data Security

MARTIN T. SHEPHERD, PARTNER

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, July 21, 2020

Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research

Indictment Alleges Two Hackers Worked With the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS), While Also Targeting Victims Worldwide for Personal Profit

A federal grand jury in Spokane, Washington, returned an indictment earlier this month charging two hackers, both nationals and residents of the People's Republic of China (China), with hacking into the computer systems of hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the United States and abroad, including Hong Kong and China. The defendants in some instances acted for their own personal financial gain, and in others for the benefit of the MSS or other Chinese government agencies. The hackers stole terabytes of data which comprised a sophisticated and prolific threat to U.S. networks.

NATIONAL SECURITY

DOJ Charges Chinese Nationals With Hacking More Than 100 Companies

September 16, 2020 · 3:40 PM ET

RYAN LUCAS

The Justice Department announced charges on Wednesday against five Chinese nationals in connection with the hacking of more than 100 American and foreign companies as well as of nonprofits and universities.

The department also charged two Malaysian businessmen with conspiring with two of the indicted Chinese nationals to target companies in the billion-dollar computer game industry. American officials say Malaysian authorities have arrested the businessmen, who now face extradition to the United States.

Deputy Attorney General Jeffrey Rosen announces the cybercrime allegations on Wednesday at the Justice Department.

Tasos Katopodis/AP

Help Net Security

Ransomware still the most common cyber threat to SMBs

Phishing, poor user practices, and lack of end user security training continue to be the main causes of successful ransomware attacks.

8 hours ago

ITProPortal

Hackers are leaning more heavily on cloud resources

Cloud enables faster and more flexible operations.

22 hours ago

PIETRAGALLO

PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP

Essential Concepts

Essential Concepts

- Information Technology
  - Critical to your practice and your clients' business
    - IT systems, networks, cloud, IoT and data
- Incident
  - An event that violates an organization's security policies and procedures
- Breach
  - Unauthorized access or loss of unencrypted personal or confidential information:
    - SSN's and DOB's
    - Bank account #'s, PINs, credit/debit card #'s
    - Medical records and treatment information
    - Access credentials: Usernames and passwords
    - Does not include information that is lawfully publicly available

- The average cost of a data breach in the U.S. was $4.24M
- Lost business is typically the highest cost (on average $1.59M)
- Detection and Escalation $1.24M
- 287 Days to Detect and Contain
- Highest costs were in the healthcare industry ($9.23M)

Ponemon Institute, 2021 Cost of Data Breach Study

Cyber Threats

What is a Cyber Threat?

- Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.

NIST Computer Security Resource Center

Spectrum Of Cyber Threats

- Hackers & other cybercriminals
- Advanced Persistent Threats (“APTs”)
- Authors of malware and phishing attacks
- Distributed Denial-of-Service attacks (“DDoS”)
- Hijacking of domain name
- Employee theft of trade secrets or IP
- Lost or stolen laptop, mobile device, USB drive
- Lax corporate security policies and systems

Verizon Threat Actions*

- Hacking – 45%
  - 80% are stolen credentials or brute force
- Social – 22%
  - 60% are stolen credentials; 10% bank records
- Error – 22%
  - Misconfiguration
    - Misconfiguration normally happens when a system or database administrator or developer does not properly configure the security framework of an application, website, desktop, or server leading to dangerous open pathways for hackers.
  - Misdelivery
    - Email misdelivery – 5th most common cause of cybersecurity breaches.
    - 58% of employees admitted to emailing the wrong person at work.

* 2020 Verizon Data Breach Report

Verizon Threat Actions*, Con ’t

- Malware – 17%
  - Varieties
    - Password dumper – 40%
    - Ransomware – 20%
  - Vectors
    - Email link or attachment – 50%
- Misuse – 8%
- Physical – 4%

* 2020 Verizon Data Breach Report

Threat Actors

- Groups
  - Organized Crime – 60%
  - Nation State – 15%
  - System Admin – 15%
- Motivation
  - Financial – 85%
  - Espionage – 15%

Cyber Threats: What are the Risks?

- Loss of online business or customers
- Loss of trade secrets, research, or IP
- Damage to brand or reputation
- Investigations by federal and state authorities
- **Civil litigation**
- **Compliance costs, including notification of affected parties**

Legal Framework
For Cyber Security

Legal Framework For Cyber Security

- Federal and state statutes
  - Set requirements for safeguarding data
  - Notification regarding data breaches
  - Civil and criminal penalties
- Federal regulations
  - Specific to federal agencies and industries
- Guidance
  - Executive Order

State Breach Notification Laws

- All States have law that requires notice of breach from organizations that collect, use, or manage personal information
- Most State Notification Laws:
  - Define a data breach
  - Identify protected data
  - Identity data that isn't protected (i.e., safe harbor)
  - Establish how & when notification is to be made
    - May depend on number of people affected and the cost of notification
- Trending
  - Require proactive data security measures to protect personal information

State Data Security Laws

- 3 primary categories:
  - “Reasonable” Data Security
    - Allows for fluid expectations as tech changes
    - Challenging for smaller organizations to obtain guidance needed
  - Specific Data Security Controls and Program
    - COBIT, NIST, CIS, ISO 27001
  - Incentive-based Affirmative Defense (OH, UT, and CT)
    - Affirmative defense to tort action for breach of duty

Industry

Health Care

- HIPAA: Health Insurance Portability & Accountability Act of 1996 - 42 U.S.C. §1320
  - Regulates the use and disclosure of “protected health information” by “covered entities”
  - A covered entity must take reasonable steps to ensure the confidentiality of protected health information - 45 C.F.R. §164.316(a)
  - Significant civil penalties under 42 U.S.C. § 1320d-5 ($100 to $50,000 per violation)
    - HHS Office for Civil Rights enforcement
  - Reasonable Security Requirement
    - Administrative, Technical, and Physical Safeguards

Health Care

- HITECH: Health Information Technology for Economic & Clinical Health Act - 42 U.S.C. §§ 17901-17953
  - Broadened HIPAA breach disclosure notification and privacy requirements to include business associates of covered entities
  - Identifies a breach & notification requirements
  - “Without unreasonable delay” but not more than 60 days
  - Notification to affected individuals, HHS, and, in certain circumstances, the media

Financial Institutions

- Gramm-Leach-Bliley Act, 15 U.S.C. 6801, 6805(b)
  - Applies to U.S. financial services organizations
  - Requires protection of the security and confidentiality of customers' non-public personal information (NPI)
  - Must provide privacy policy to customers
    - Customers can opt out of disclosure of NPI to third parties
    - Safeguards to protect NPI
  - Protection should be "appropriate to the size and complexity of the bank and the nature and scope of its activities"
  - Interagency Guidance Establishing Standards for Safety and Soundness - 12 C.F.R. §364

Defense Industrial Base

DFARS, NIST 800-171, Cybersecurity Maturity Model Certification (CMMC)

- DFARS/NIST
  - Protect CUI and FCI
  - Self assessment of cyber controls
- CMMC-AB ecosystem of standards and professionals
  - Based on DFARS and 800-171
  - 5 Level progressive maturity
  - RP and RPOs
  - Audited assessment by certified auditors (C3PAO)
  - 2025 Full program implementation

Guidance

Guidance

- Presidential Executive Order on Improving the Nation's Cybersecurity, May 2021
  - Remove Barriers to Threat Information Sharing Between Government and the Private Sector
  - Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
  - Improve Software Supply Chain Security
  - Establish a Cybersecurity Safety Review Board
  - Create a Standard Playbook for Responding to Cyber Incidents
  - Improve Detection of Cybersecurity Incidents on Federal Government Networks
  - Improve Investigative and Remediation Capabilities

NIST

Search NIST

Menu

NEWS

NIST Offers ‘Quick-Start’ Guide for Its Security and Privacy Safeguards Catalog

Companion to recently updated controls catalog provides useful starting points for risk management.

October 29, 2020

Credit: Shutterstock/K. Kalchenko

MEDIA CONTACT

Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

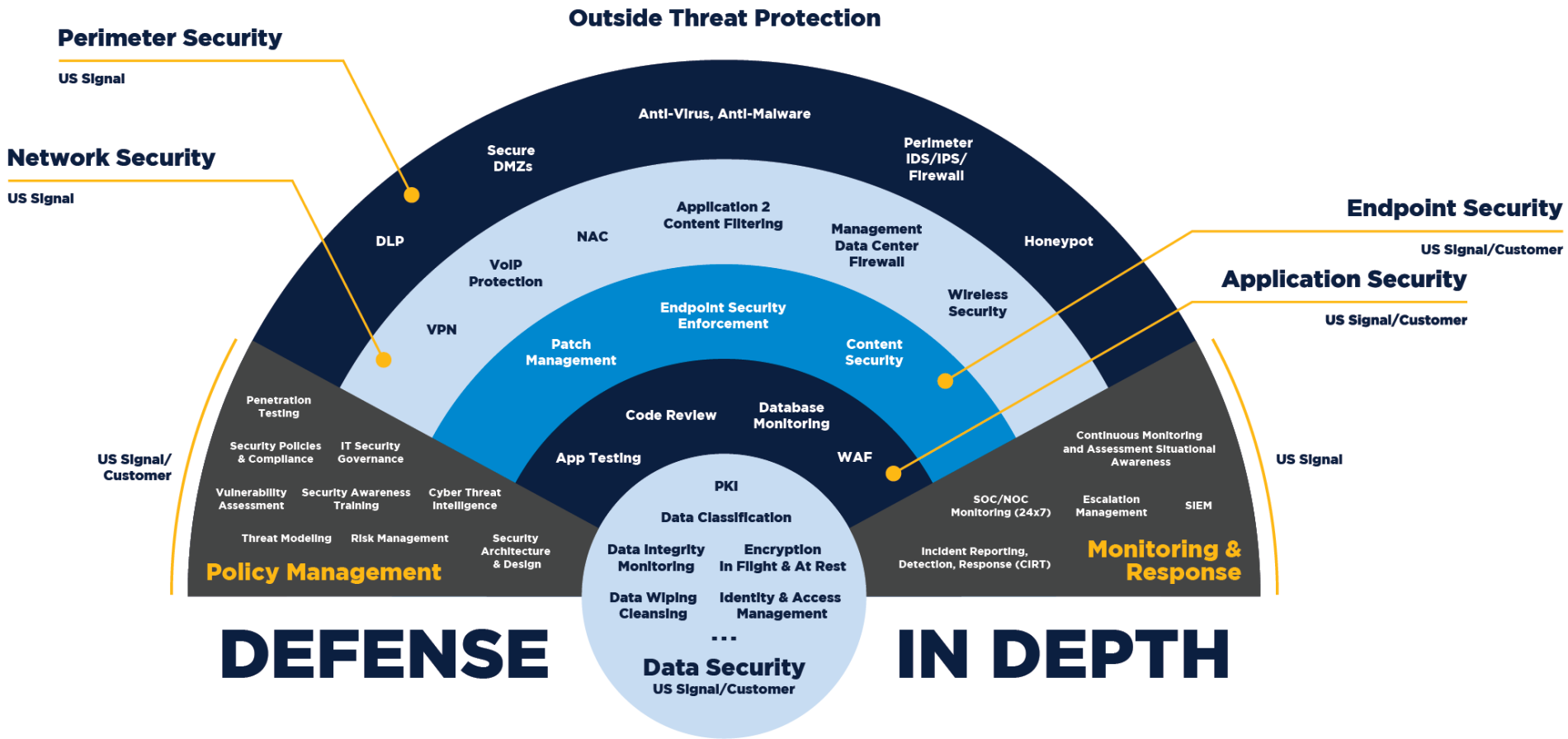
ORGANIZATIONS

Information Technology Laboratory
Computer Security Division
Computer Security - HQ

RELATED LINKS

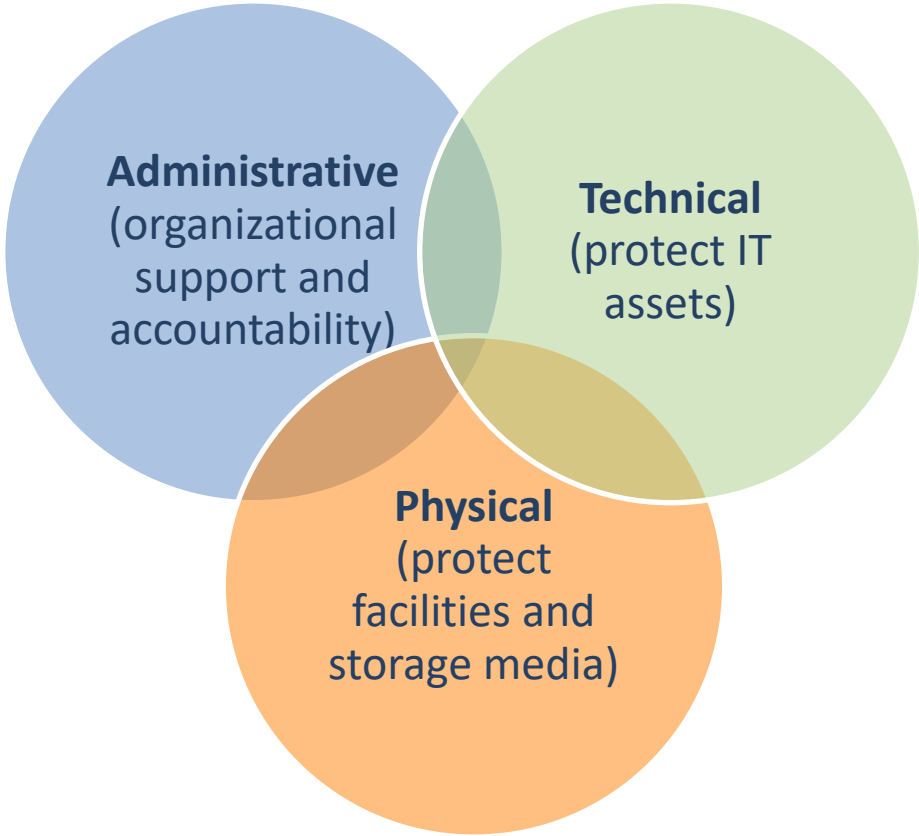
https://www.nist.gov/news-events/news/2020/10/nist-offers-quick-start-guide-its-security-and-privacy-safeguards-catalog

Safeguards as Best Practice


Outside Threat Protection
Perimeter Security
US Signal
Network Security
US Signal
Endpoint Security
US Signal/Customer
Application Security
US Signal/Customer
Anti-Virus, Anti-Malware
Secure DMZs
Perimeter IDS/IPS/ Firewall
DLP
NAC
Application 2 Content Filtering
Management Data Center Firewall
Honeypot
VoIP Protection
Wireless Security
VPN
Endpoint Security Enforcement
Patch Management
Content Security
Code Review
Database Monitoring
App Testing
WAF
PKI
Data Classification
Data Integrity Monitoring
Encryption In Flight & At Rest
Data Wiping Cleansing
Identity & Access Management
...
Data Security
US Signal/Customer
US Signal/ Customer
Penetration Testing
Security Policies & Compliance
IT Security Governance
Vulnerability Assessment
Security Awareness Training
Cyber Threat Intelligence
Threat Modeling
Risk Management
Security Architecture & Design
Policy Management
US Signal
Continuous Monitoring and Assessment Situational Awareness
SOC/NOC Monitoring (24x7)
Escalation Management
SIEM
Incident Reporting, Detection, Response (CIRT)
Monitoring & Response
DEFENSE IN DEPTH

Safeguards

Three key types of interrelated safeguards include:



Safeguards– Common Elements

- Technical
  - Firewalls
  - Rule-based authentication
  - Password management an MFA
  - Anti-virus
  - SIEM
- Administrative
  - Written policies and plans
  - Vendor management
  - Employee Training
- Physical
  - Badging credentials
  - Visitor management

Other Best Practices

- Multi-faceted approach:
  - Strong security policy and firm implementation plan
  - Sensible, effective technical controls
  - Security culture
  - Insurance – know what is covered
  - Annual “audit”
  - Manage vendor risk

Christopher A. Iacono

Christopher A. Iacono is a Partner in the Philadelphia office of Pietragallo Gordon Alfano Bosick & Raspanti, LLP. He practices in the Cybersecurity & Privacy; Government Enforcement, Compliance, and White Collar Litigation; Health Care; and Commercial Litigation Practice Groups.

Mr. Iacono focuses his litigation practice on commercial litigation, white collar criminal defense, internal investigations, compliance, health care litigation, and professional licensing litigation.

Mr. Iacono regularly represents government or private institutions and individuals before local, state, and federal grand juries. He has conducted dozens of internal investigations related to fraud and abuse issues, ethics violations, NCAA violations, Title VII violations, and Title IX violations. He also has extensive experience concerning a myriad of legal issues relevant to representing target, subject, and witnesses in grand jury proceedings.

Contact Info:
(215) 320-6016 CAI@Pietragallo.com

Bar Admissions:
- Pennsylvania
- New Jersey

Education:
- J.D., *magna cum laude*, Widener University School of Law
- B.A., Ursinus College

Martin T. Shepherd

Martin T. Shepherd is a well-known innovator in cybersecurity and privacy and an accomplished litigator. He brings his clients considerable experience as a litigator, in-house counsel, and as the founder and CEO of Arch Access Control and Arch Canopy, Inc., organizations committed to ending a companies' exposure of loss due to physical or cyber security breach. He is also former in-house counsel at EQT Corporation in Pittsburgh, PA. Mr. Shepherd leads the firm's Diversity Initiative and is a member of the Cybersecurity & Privacy Group.

Mr. Shepherd advises major businesses on a wide range of cybersecurity and privacy legal, policy, and investigative matters, including a strategy to identify and address companies' cybersecurity compliance demands. He conducts assessments and integrates security technology solutions which include a full array of physical and cyber technology.

He has handled cases involving real estate and contract disputes, business torts, civil rights, trademark, and medical malpractice. Mr. Shepherd also has considerable experience as an in-house attorney at a Fortune 500 Company.

Contact Info:
(412) 263-1814
MS1@Pietragallo.com

Bar Admissions:
- Michigan

Education:
- Certificate in Executive Leadership, Carnegie Mellon University Tepper School of Business
- J.D., Ohio State University Moritz College of Law
- B.S., Miami University

5
Offices

55+
Attorneys

78%
Attorneys have over
7 years of practice

71%
Attorneys have
real trial experience

Your Future. Our Business.

Since the founding of our firm in 1987, we have measured our success by generating proven results time-and-again for our clients. From the boardroom to the courtroom, our attorneys combine industry knowledge with legal expertise to devise a strategy and develop a solution for your unique need.

Results Matter Most

Our clients range from Fortune 200 and large privately-held companies to municipal entities, small businesses and partnerships in a broad diversity of industries and business sectors. With each representation, our attorneys work to ensure that matters are addressed practically and efficiently, and in a manner best suited for you. At Pietragallo, ***results matter most***.

PIETRAGALLO
PIETRAGALLO GORDON ALFANO BOSICK & RASPANTI, LLP