Data Privacy and Security

December 17, 2019

Kirsten Bay
cysurance

Angelo A. Stio

Peter J. Wakiyama
Pepper Hamilton LLP
Attorneys at Law

Moderated by
Gregory J. Nowak

Overview

- Data and ownership
- Data protection
- SEC Cybersecurity
- Cyber insurance

Data and Data Ownership

- What is “data”?
- Is data capable of being owned?
- Do property rights exist in data?
- Does anyone really own data?

Data and its Value is Driving the Digital Economy

- Data is driving the digital economy
- Data is valuable and increasing in value as greater quantities can be stored and analyzed
- Issues concerning data are often framed around “ownership” or “property rights”

Before Digitization

- Going back in time, before computers and digitization, data, if captured, appeared in a tangible medium
- The data or information expressed in a letter or other document existed separate from the tangible medium
- The tangible medium is capable of being owned as a form of property, but the information is not subject to the same legal principles

Property Rights

- What is the concept of ownership
  - Exclusive use or monopoly
  - Right to dispose of or convey
- Types of property
  - Real property
  - Personal property
  - Intellectual property

No Place for Data in a Property World?

- No known “data property law” or “data ownership law” anywhere in the world
- Data is not real property
- Data is not personal property
- What about intellectual property?

Data as Intellectual Property?

- **Trade secret** - protects against misappropriation; subject matter loses protection if disclosed to the public or becomes known to others without restriction; does not grant "exclusive" rights (unlike copyright); more like tort law than property law
- **Copyright** - protects only the creative expression, and not the information; no protection for facts; creative compilations of data may be protected, but not the data contained within the compilation or a database

Data as Intellectual Property?

- **Patent** - protects new, novel, non-obvious and useful inventions, but not the underlying data; in fact, when published, the data is available to the public, so whatever trade secret protection existed is also extinguished
- **Trademark** - protects the trademark (e.g., product name) from use in a confusingly similar manner; does not grant any ownership rights in the data or information pertaining to the name or the goods or services associated with the name

Parties Routinely Enter into Agreements Concerning Data Ownership

Doesn't that Demonstrate Ownership of Data?

- Under contract law, parties can convey exclusive rights, agree to restrictions and generally agree between or among themselves concerning "ownership" of data
- These arrangements are similar to rights conferred under property laws
- However, these rights are limited to the contracting parties
- These rights are not actual property rights and are not equivalent to property rights afforded under law

Do Data Privacy Laws Provide for Data Ownership and Protect Data Owners?

- No, data privacy laws grant data subjects the right to exclude others from using certain personal information about them
- These data privacy rights are similar to property rights that allow one to exclude or prevent others (for example, copyrights), but are not equivalent
- Unlike property laws (for example, copyrights), data privacy laws do not incentivize creation

Where Does that Leave Individuals and Businesses?

- Under existing laws, no one owns data
- Existing intellectual property laws may provide some limited forms of protection, but not ownership
- Addressing rights and restrictions between parties in contracts is critical
- Data privacy cannot be equated with ownership
- Future legislation may address data ownership rights

Two Approaches to Data Privacy and Security

- United States
  - Sectoral Approach
    - Mix of federal and state laws based on industry, data subject and data type, rather than one comprehensive data privacy and security law
- International
  - Omnibus Approach
    - General approach is to have one broad, overarching data privacy and security law

Pepper Hamilton LLP
Attorneys at Law

What is PII?

- Personally Identifiable Information (PII) is any information relating to an identified or identifiable natural person
- PII includes any piece of information which can be used to uniquely identify or trace an individual's identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual
- Courts are recognizing that "anonymized" data may be recombined to obtain PII
- "Sensitive" PII
  - Certain data elements, such as financial and medical information, may be more highly regulated and receive heightened protection under particular laws

What is PII?

Common Data Elements

- Full name
- Personal identification numbers
  - *e.g.*, national identification number, driver's license number, passport number
- Biometric records
  - *e.g.*, finger prints, retina scans, handwriting samples, voice prints
- Credit card and financial account numbers
- Date of birth
- Telephone number
- Street address
- Zip code
- Email address
- Digital identifiers
- Demographic information
  - *e.g.*, gender, age, race or ethnic origin
- Medical or health information, including accommodations
- Religious beliefs or affiliation
- Political opinions
- Ratings or test scores

Pepper Hamilton LLP
Attorneys at Law

Federal Statutory Protections

Unfair or Deceptive Trade Practices

- **FTC Act** - The FTC has broad authority under the FTC Act to enforce against "unfair or deceptive" trade practices
  - With exceptions for certain industries, the FTC has general responsibility for regulating data privacy and security
  - In the data privacy and security space, the FTC investigates trade practices such as:
    - Failure to comply with privacy policies
    - Failure to implement industry standard data security measures

Federal Statutory Protections

Advertising and Marketing

- **Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)** - Regulates the content, format, labeling and sending of commercial messages to businesses and consumers
  - Commercial if "primary purpose" is "commercial advertisement or promotion of a commercial product or service"
  - Applies to emails and some text messages
  - Must avoid false or misleading messages and obtain the recipient's consent
- **Telephone Consumer Protection Act (TCPA)** - Regulates the making of telemarketing calls and the use of automatic dialing systems and artificial or prerecorded voice messages
  - Applies to calls, text messages and faxes
  - Do-Not-Call registry

Federal Statutory Protections

Financial Privacy

- **Gramm-Leach-Bliley Act (GLBA)** - Regulates financial institutions' treatment of personally identifiable financial information
  - "Financial institutions" is broadly defined—companies that offer financial products or services to individuals
- **Fair Credit Reporting Act (FCRA)** - Regulates the use of PII contained in consumer reports by consumer reporting agencies (CRAs), furnishers of PII to CRAs and users of consumer reports

State Statutory Protections

- All 50 states and Puerto Rico have data breach notification laws that generally seek to prevent identity theft
- Some state statutes offer broader protection of PII than federal laws
  - *e.g.*, California and Massachusetts
- Rapidly evolving regulatory landscape
- Federal privacy laws generally do not preempt state laws

California Consumer Privacy Act (CCPA)

- Broad exposure - personal information / sale
- Consumer rights
  - Right to Know
  - Right to Deletion
  - Right to Opt-Out of “Sale”
  - Right to be Free from Discrimination
- Effective January 1, 2020
  - Private right of action for data breaches
  - Enforcement by the Attorney General July 1, 2020

International

EU

- Comprehensive law is typical approach outside of U.S.
- General Data Protection Regulation (GDPR)
  - Replaces current “Directive” May 25, 2018
  - Fines up to the higher of 4% of global revenue or €20M
  - 72 hour breach notification
  - Mandatory data protection officers
- Cross-Border Data Transfer
  - Model contractual clauses
  - Privacy Shield
  - Binding Corporate Rules
  - Consent
- UK - Brexit

Pepper Hamilton LLP
Attorneys at Law

International

Canada

- Federal Law: Personal Information Protection and Electronic Documents Act (PIPEDA)
  - General Rule: No collection, use or disclosure of personal information without consent
  - Notice; appropriate security; breach notification requirement (not yet in force)
- Provincial Laws
  - BC, Alberta, Quebec
  - Data breach notification – Alberta
- Canadian Anti-Spam Law (CASL)
  - No email marketing messages without express or implied consent
  - Consent only implied for past customers for 2 years
  - Private right of action comes into force July 1, 2017

Practical Privacy Compliance

Legal Requirements

- Provide appropriate notices
- Observe any applicable legal restrictions on collection and use
- Obtain appropriate consents for collection (e.g., geo-location, biometrics, other sensitive data) and for marketing uses
  - Opt-in/Opt-out
  - Properly manage preferences
- Exercise appropriate diligence when selecting vendors and appropriate oversight during relationship with vendors
- Ensure vendor contracts include appropriate data ownership, data use/license, data security, cybersecurity insurance and indemnification clauses
- Notify individuals in the event of a security breach that compromises certain personal information

Practical Privacy Compliance

Privacy Policies

- Privacy concepts addressed in internal/external policies
- Legal Requirements
  - **California Online Privacy Protection Act (CalOPPA)** - requires online privacy policies (de facto national standard for online privacy)
  - **Federal FTC Act and State Unfair and Deceptive Acts and Practices (UDAP) Statutes** - Under these statutes public privacy policies are legally binding promises, enforceable by FTC and State AGs
  - **GLBA** - Financial institutions are required to provide consumer privacy notices
  - **CCPA** - Requires special notice to California residents regarding consumer CCPA rights and the online and offline collection, use and disclosure of personal information by a business

Practical Security Compliance

FTC Start with Security Guidance

Lessons learned from 50+ data security related enforcement actions

- Start with security
- Control access to data sensibly
- Require secure passwords and authentication
- Store sensitive personal information securely and protect it during transmission
- Segment your network and monitor who is trying to get in and out
- Secure remote access to your network

- Apply sound security practices when developing new products
- Make sure your service providers implement reasonable security standards
- Put procedures in place to keep your security current and address vulnerabilities that may arise
- Secure paper, physical media, and devices

Pepper Hamilton LLP
Attorneys at Law

Practical Security Compliance

Legal Requirements

- **FTC Act** - Failure to implement "reasonable" security as an "unfair" trade practice. (See Start with Security)
- **Massachusetts (201 CMR 17.00)** - Requires written information Security program (WISP) and specific IT-related security measures
- **GLBA** - Requires financial institutions to have measures in place to keep customer information secure
- **Other state laws**
  - State breach notification laws often exempt encrypted data
  - Require vendor contracts to address security
- **Privacy Policy Security Representations** - Legally enforceable under FTC Act and State UDAP statutes

Risks and Potential Liability

- FTC Enforcement (Fines, Consent Decrees)
- AG Enforcement (Fines, Injunction)
- Private causes of Action
  - Lawsuits following data breach
  - Shareholder derivative suits
  - TCPA
  - Illinois Biometric Information Privacy Act
  - CCPA

Monetary Loss

- Data breach costs averages $242 per record in U.S.
  - Forensics; legal; PR; notification; loss of business; employee time
- Litigation
  - ***Curry v. AvMed*** - laptop theft; 1.2M class members; settled for $3M
- Brand Damage

- Fines and penalties
  - **Wyndham** - 20 year consent decree requiring comprehensive information security program to protect payment card data, including annual audits
  - **InMobi** - $950K FTC settlement for deceptively tracking consumer locations
  - **CVS/Caremark** - $2.25M FTC settlement for improper disposal of data
  - **Choice Point** – FTC settlement of $15M regarding sale of customer information
  - **Lifelock** - $100M to settle FTC contempt charges that it violated 2010 settlement by continuing to make deceptive claims about services

Takeaways

- Accountability is important at all levels
- Analyze proposed new uses, collections and disclosures of personal information for compliance
- Limit collection, access and transfer where possible
- Securely handle devices and paper containing personal information
- Be wary of social engineering

Takeaways

- Be cognizant that you will be held responsible for the privacy policy you publish
- The obligation to timely warn is as important as the duty to protect
- Conduct appropriate diligence and oversight of vendors
- Protect data assets, including physical, technological and legal protections
- Ensure compliance by third parties, including vendors
- Document compliance steps

The “Bitter C-Suite”: Privacy, Security and Data Protection Issues Facing Corporations, Directors and Officers

Pepper Hamilton LLP
Attorneys at Law

Officer and Director Liability

- Directors are liable for oversight of Company affairs due to their fiduciary duties of loyalty and due care
- Cyber liability due to disclosure of personally identifiable information and trade secrets are known material risks
- Standard of Care as to cyber liability generally can be categorized into regulations dealing with:
  - Duty to warn
  - Duty to protect

Duty to Warn

- SEC Guidance
- Data breach laws and regulatory requirements

Duty to Warn: SEC Guidance

Division of Corporation Finance

Securities and Exchange Commission

CF Disclosure Guidance:

Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

SEC Guidance

Rationale

- Increased dependence on digital technologies to conduct operations
- Increased risk associated with cybersecurity
- More frequent and severe cyber incidents
- Recent increased focus on how risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities law

SEC Guidance

Cyber Incidents

- Cyber incidents may be:
  - Deliberate attacks; or
  - Unintentional events
- Cyber incident results:
  - Misappropriating assets or sensitive information;
  - Corrupting data;
  - Causing operational disruption; or
  - Denial-of-service on websites.
- Cyber attacks may range from:
  - Highly sophisticated efforts to electronically circumvent network security;
  - Highly sophisticated efforts to overwhelm websites; or
  - More traditional intelligence gathering information necessary to gain access.

SEC Guidance

Remediation Costs

- Remediation costs can be substantial with negative consequences including, but not limited to:
  - Liability for stolen assets or information
  - Repairing system damage that may have been caused
  - Increased cybersecurity protection costs
  - Lost revenues resulting from unauthorized use of proprietary information
  - Lost revenues from failure to retain or attract customers following an attack;
  - Litigation; and
  - Reputational damage.

SEC Guidance

Disclosure

- Cybersecurity risks and cyber incidents are required to be disclosed when:
  - Necessary in order to make other required disclosures not misleading
  - They are such that a reasonable investor would consider important to an investment decision
- No existing specific disclosure requirement
  - Registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents

SEC Guidance

Disclosure

- Registrants should:
  - disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky;
  - consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks; and
  - consider the adequacy of preventative actions taken to reduce cybersecurity risks
- Registrants are not required to disclose information that would help potential attackers

SEC Guidance

Disclosure

- Places reporting companies may need to include disclosure:
  - Risk factors
  - MD&A
  - Description of the business
  - Legal proceedings
  - Financial statement disclosures
  - Disclosure controls and procedures

SEC Guidance

Disclosure

- Is a Form 8-K required after a breach? No (not yet)
- Some companies have elected to file under item 8.01 (Other Information)
- Some companies have taken the position that they notify the public of a breach in other ways and an 8-K is unnecessary
  - Pros: Eliminate any potential insider trading, don't raise flags with the SEC, disclosure can be copied from breach notices
  - Cons: Imperfect information

RIAs and Brokers-Dealers: Recent Risk Alerts Highlight Privacy and Security Issues

Pepper Hamilton LLP
Attorneys at Law

Background

- Privacy and security compliance is required under Regulation S-P
- Cybersecurity is one of the SEC's main areas for examinations

Areas of Focus

- Proper configuration of network storage devices
- Information security governance
- Policies and procedures

April 16 Risk Alert

- Privacy and Opt-Out
  - Under Reg. S-P., registrants must deliver “clear and conspicuous” notice regarding privacy policies and practices
  - Must inform customers of “opt-out” rights from disclosures to unaffiliated third parties
  - Examined entities frequently fail to provide such notices or provide inaccurate or incomplete notices
- Safeguards Rule
  - Registrants must adopt written policies and procedures addressing administrative, technical and physical safeguards
  - SEC has found lack of policies and procedures; policies not implemented; policies not reasonably designed to ensure protection of customer data

May 23 Risk Alert

- Customer Records in Network Storage
  - Alert focused on entities that used cloud-based storage solutions from third party service providers
  - Emphasized importance of encryption and password protection
  - Three areas of concern covered:
    1. Misconfigured network storage solutions – inadequate configuration of security settings
    2. Inadequate oversight of vendor-provided network storage
    3. Insufficient data classification policies and procedures

Conclusion

- RIAs and brokers-dealers must take adequate steps to meet privacy and security obligations:
  - Design and actively maintain policies and procedures – customer notice, access controls, vendor management, information security governance
  - Periodic cybersecurity audits – vulnerability assessments, penetration testing – to ensure standards are being met internally and among third party service providers

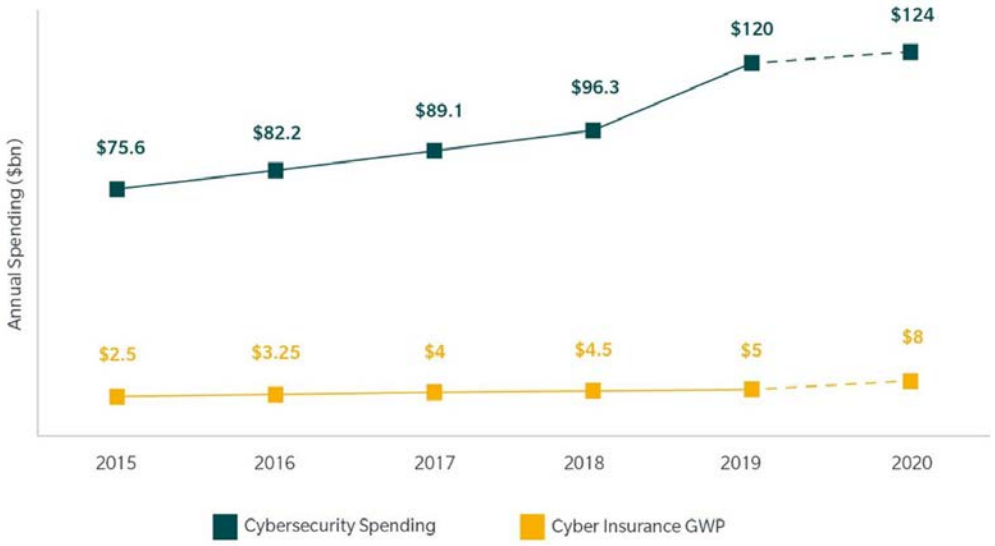
Cyber Insurance and Risk Management

Pepper Hamilton LLP
Attorneys at Law

The Insurance Adoption Conundrum

Cysurance believes the cyber risk management trifecta consists of robust cybersecurity, strategic planning, and comprehensive cyber insurance. To date, insurance adoption has significantly lagged technology implementation and strategic planning.

- Since 2016, Chief Information Security Officer budgets have grown from 7.1% of overall IT budgets to 9.5%
- In the next three years:
  - 67% of organizations plan to invest more in cybersecurity technology and mitigation
  - 53% plan to increase spending on staff training
  - 40% will invest more in cyber event planning and preparation
  - 34% will increase spending on cyber insurance



Despite this trend, cyberattacks tripled among small businesses from 2015 to 2019. And though 54% of businesses believe a cyberattack or data breach is inevitable, nearly half do not carry cyber insurance!

cysurance

Protect, Detect, Remediate

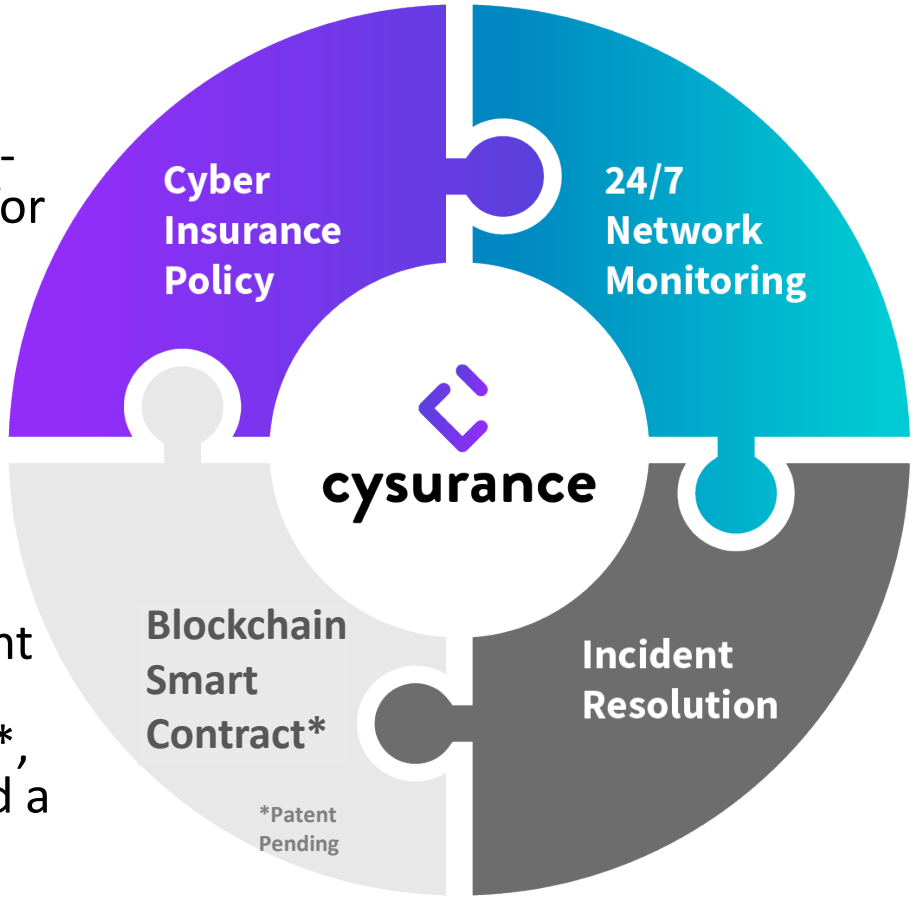
- By integrating cybersecurity technology, cyber governance and cyber insurance, SMBs achieve holistic cyber risk management that:
- Leverages regulatory guidance to provide a roadmap for technology investments and strategic planning
- Identifies and targets digital assets for heightened protection and/or insurance coverage
- Supports insurance payouts by documenting compliance efforts and the satisfaction of policy conditions
- Indemnifies SMBs not only for ransomware or damaged hardware, but also the more severe costs associated with business interruption and incident response.

cysurance

Cysurance – Cyber Insurance as a Service

Our **proprietary policy** eliminates applications and underwriting and ensures **comprehensive protection** for potentially catastrophic first **AND** third-party losses. It is designed and priced for SMBs and distributed through their commercial lenders and third-party service partners to reduce friction and encourage adoption.

Using SMBs' existing network monitoring technology or our proprietary **mini-sensor**, Cysurance detects threats in real time. In the event of an attack, proof of breach is irrevocably recorded in the blockchain*, **automatically triggering the policy** and a dedicated breach response team and creating full transparency between parties.



cysurance

Questions & Answers

Kirsten Bay

Co-Founder and CEO
Cysurance

Kirsten Bay brings over 25 years of experience in risk intelligence, information management, and policy expertise across a variety of sectors. In the last 6 years, Kirsten has been the CEO of big data and cyber security companies, leading the strategy and development of next generation analytics and attack detection technologies.

Throughout her career, Kirsten has been appointed to congressional committees developing cyber policies, initiatives and recommendations for the intelligence community and held executive roles at Cyber adapt, Attensity Group, and iSIGHT Partners.

cysurance

Angelo A. Stio

Partner, Trial and Dispute Resolution
Pepper Hamilton LLP

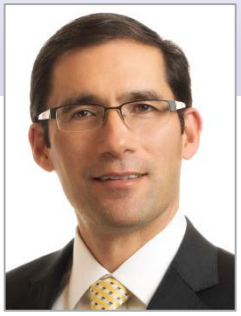
609.951.4125 / 212.808.2700 | stioa@pepperlaw.com

Angelo, a seasoned trial attorney who has litigated and arbitrated in courts and before arbitration panels throughout the United States, helps clients achieve their litigation goals through the development of a factual record and the effective presentation of arguments through motion practice and trial advocacy.

Some of his recent engagements include defending a publicly traded company in a class action arising from a data breach, defending a client in a shareholder class action alleging violations of Section 10(b) of the Securities Exchange Act of 1934 and Rule 10(b)(5), representing a client in the pursuit of claims under the terms of a manufacturing and sales agreement and Article 2 of the Uniform Commercial Code, and defending hedge fund clients against claims asserted by limited partners.

During the course of his career, Angelo also has developed a deep understanding of federal and state laws related to data privacy and security. He is a co-chair of the New Jersey Bar Association Privacy Law Committee and is designated as a Certified Information Privacy Professional on U.S. laws (CIPP/US) by the International Association of Privacy Professionals.

Pepper Hamilton LLP
Attorneys at Law



Peter T. Wakiyama

Partner, Intellectual Property
Pepper Hamilton LLP
215.981.4538 | wakiyamp@pepperlaw.com

Peter focuses his practice on intellectual property and technology law, including intellectual property and technology transactions; general counseling, protection, enforcement and commercialization of intellectual property rights; information technology; Internet and e-commerce matters; data privacy and security; and media/new media/social media, publishing, entertainment and the arts.

He has represented a wide range of domestic and international clients across many industries, including software, Internet/e-commerce, telecommunications, cable television, entertainment, financial services, manufacturing, fashion, retail, health care, consumer packaged goods, packaging, food and beverage, education, hospitality and real estate (residential and commercial).

Pepper Hamilton LLP
Attorneys at Law

Gregory J. Nowak

Partner, Financial Services
Pepper Hamilton LLP
215.981.4893 / 212.808.2723 | nowakg@pepperlaw.com

Greg concentrates his practice in securities law, particularly in representing investment management companies and other clients on matters arising under the Investment Company Act of 1940

He represents many hedge funds and other alternative investment funds in fund formation and investment and compliance

Greg has represented a broad range of investment funds and fund managers with products spanning both the private equity and hedge fund markets.

He writes and speaks frequently on issues involving investment management, health care and other matters and is the author of five books on hedge funds.

Pepper Hamilton LLP
Attorneys at Law

For more information, visit

www.pepperlaw.com

Peter T. Wakiyama

Pepper Hamilton LLP

Pepper Hamilton LLP
Attorneys at Law