# LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

## Introducing PilieroMazza's Cybersecurity and Data Privacy Practice

By Jon Williams

We are very excited to present this special cybersecurity-focused issue of the *Legal Advisor* as our first issue of 2019 and the first issue under our new editor, **Michelle Litteken**. Cybersecurity and data privacy have been increasing focal points for Congress, federal agencies, and contractors in recent years. We have been tracking these developments closely and expect these trends will only intensify in 2019.

Cybersecurity awareness and preparedness are critical for federal contractors, not just as a matter of compliance, but also to gain (or avoid losing) a competitive advantage. The U.S. Department of Defense (DoD) is moving forward with cybersecurity as the fourth pillar of its acquisition decision-making, and civilian agencies are increasingly following DoD's lead by including cybersecurity as an evaluation factor in solicitations and contract awards. The General Services Administration (GSA), for one, has new cybersecurity rules in the works and will make more regular use of cybersecurity in its source selection decisions this year.

As you'll see in this issue, cybersecurity can impact a company in a multitude of ways. For example, cybersecurity can affect corporate transactions. As **Kathryn Hickey** and **Dave Shafer**, explain in their article "Managing Cyber Risks in M&A Transactions," cybersecurity is a consideration for contractors looking to sell their firms. Cybersecurity is also a concern from an employment perspective. In their article, "Hackers Are No Match for Employee Missteps," **Nichole Atallah** and **Tony Batt** provide recommendations for how companies can prevent employee data breaches. If there is a breach, litigation may follow. In "When Hackers Attack: Disclosure Obligations and Litigation Risks When You Suffer a Data Breach," **Matthew Feinberg** and **Emily Rouleau** discuss laws related to data breaches and how to respond to a breach. Finally, **Cy Alba** weighs in on the intersection between data rights and breaches in "Data Breaches and Data Rights: How the Rights of You and Your Customers Are Impacted."

The integral and growing role that cybersecurity and data privacy requirements play for federal contractors led us to form our new **Cybersecurity and Data Privacy Practice**, which we are proud to launch this year. PilieroMazza's Cybersecurity and Data Privacy Practice pulls together lawyers from across all of our practice groups to advise and assist clients with a comprehensive approach to managing cybersecurity, information privacy, and data protection risks; establishing compliant and effective safeguards; and responding to cybersecurity and privacy incidents when they do occur. This practice provides a broad range of services to federal contractors and commercial firms, including analysis of cybersecurity compliance under the NIST Framework; review and development of information security programs, including preparation of employee and personnel related handbooks and training; data breach incident response policies and procedures, tabletop exercises,

## Special Cybersecurity Issue



*Continued on page 2*

PILIERO MAZZA

## DATA PRIVACY PRACTICE ..Continued from page 1

and management training; assistance with breach response management, including governmental and customer notifications, governmental investigations, and audits; breach litigation strategy and defense, including class action and shareholder derivative suit defense; cybersecurity diligence and negotiation in mergers, acquisitions, and other corporate transactions; review and development of contract templates and federal contract "flow down" provisions to address cybersecurity requirements applicable to vendors; preparation and submission of variance requests, requests for equitable adjustment, and contract claims to procuring agencies related to cybersecurity requirements in federal contracts, and much more.

We are also rolling out a new **Cybersecurity Compliance Check-Up**. The Check-Up is a unique flat-rate offering for federal contractors designed to provide a quick assessment of the federal cybersecurity requirements applicable to your company, your current level of compliance, and steps to take to fill any gaps in your current cybersecurity practices. To learn more about the Check-Up and our new Cybersecurity and Data Privacy Practice, please visit our website at https://www.pilieromazza.com/cybersecurity.

Finally, we will be hosting a **cybersecurity and supply chain risk management event** later this year in the Washington, DC area. Stay tuned for more details on this event soon.

In closing, a lot is happening with cybersecurity and we will remain at the forefront. We hope you enjoy this special issue and will contact our Cybersecurity and Data Privacy Practice when you have a need in this area.

**About the Author:** Jon Williams is a partner and a member of the Government Contracts Group. He may be reached at jwilliams@pilieromazza.com.

### ● ● ● Announcing Our New Editor ● ● ●

Michelle Litteken

We welcome our new editor of The *Legal Advisor*, **Michelle Litteken**, and would like to thank our outgoing editor, **Jon Williams**, for his over ten-year leadership of the newsletter. Jon has made a vital contribution over the years to the quality of each edition and mentorship of our authors. He will move on to other leadership roles in the firm and is leaving the publication in very good hands. Michelle has the knowledge and dedication to help PilieroMazza remain a thought leader in our major practice areas of government contracts, business and corporate law, labor and employment, and litigation. ●

## Managing Cyber Risks in M&A Transactions

By Kathryn Hickey and Dave Shafer

No company or industry is immune from cyber risks. With an increasingly digitized marketplace, proprietary company data, as well as the sensitive data of your customers and employees, is an attractive and often easy target for bad actors looking to profit from exploiting a company's vulnerabilities. While cybersecurity concerns are significant in the daily operations of a company, in the M&A deal context, they take on a particular importance because of the material impact cyber vulnerabilities can have on a buyer's risk and therefore deal pricing. A buyer in any acquisition will want to understand the full scope of a target's cyber infrastructure and risk for exposure to take steps in the definitive agreement and deal negotiations to address identified areas of exposure and develop a plan mitigate those risks post-closing. Conversely, the seller will want to get ahead of any cyber issues in order to avoid prolonged negotiations and potential decreases in company valuation due to the identification of exposure resulting from data breaches or failure to be in compliance with applicable law or industry standards. Getting ahead of potential issues early can save time and money for both parties in a transaction and avoid, as much as possible, any post-closing surprises.

One need not look any further for an example than the recent discovery that Marriott International inadvertently purchased a reservation database that had been previously compromised, with the unauthorized third-party still in the database undetected as of closing, during its merger with Starwood Hotels in 2016. The discovery occurred post-closing, shifting the exposure to Marriott, as opposed to a similar incident wherein Yahoo! discovered a similar breach prior to closing on a sale of its assets to Verizon Communications and thereby giving the parties the ability to leave the exposure with Yahoo! The comparison between these two situations is a perfect illustration of the value of thorough cyber diligence and its impact on a buyer's ability to mitigate post-closing exposure due to compromised seller systems. This article sets forth the framework for "best

*Continued on page 3*

practices" in cyber M&A diligence and how parties can utilize these strategies in negotiating and closing deals.

## Due Diligence — Assessing Cyber Risk

At the outset of any deal, a buyer should include in its diligence of the target company an effort to understand the target's cybersecurity systems, programs, policies, and standards to evaluate potential risk of breach. A key component of this evaluation is identifying the types of sensitive data that may be exposed due to any deficiencies in cyber protections. Sensitive information can include consumer credit card and financial information, personally identifiable information of employees and customers, biometrics, protected personal health information, internal company intellectual property, other proprietary information, customer lists, third party proprietary information, and government sensitive or secure data. Appreciating the types of information that could be vulnerable to a cyber-attack can inform the buyer's effort to determine the likely severity, legal exposure, and cost of a breach.

**"Getting ahead of potential issues early can save time and money for both parties in a transaction and avoid, as much as possible, any post-closing surprises."**

Related to the question of the type of sensitive information held by the target is the question of whether the target maintains compliant, secure systems at a level appropriate for the data it manages. A systems diligence team should evaluate protections at all systems levels in order to identify vulnerabilities or insufficiencies. This process can also evaluate the target's existing cyber infrastructure, including systems and policies, to confirm compliance with industry cybersecurity standards. While industry recommended standards do not ensure protection from breach, they can be an important benchmark in determining the reasonableness of a seller's existing cyber practices. Diligence at this level should also include a review of the target's internal policies and procedures, breach response practices, and internal audits and controls.

The technical cyber diligence should also focus on identifying prior or existing breaches impacting the target and understanding the scope and potential damages associated with that breach. It is important to answer certain key questions in evaluating known breaches:

- When and for how long did the breach occur? Is there evidence or knowledge of any continuing breach?
- What information was compromised? Were copies made? Were changes made to the target's systems or files?
- Were measures taken to resolve vulnerabilities following the breach? Are they sufficient?
- Was there compliance with all required notifications/reporting requirements upon discovery of the breach?
- Are there potential claims by third parties resulting from the breach? Is there a likelihood of any shareholder derivative suit or class action?
- Did the breach create grounds for a "for cause" termination under any material contracts of the seller?

In answering these types of questions, a buyer can attempt to put boundaries around known breaches and any continuing liabilities for an acquirer of the seller.

The complementary component to diligence of a target's cyber systems and programs is diligence of the target's existing contracts from a cyber risk allocation perspective. In reviewing a target's vendor contracts or subcontracts, a buyer and their legal team should focus on determining who bears the contractual responsibility for ensuring the security of electronic data that vendors access, control, or manage. If security is the vendor's responsibility, a buyer should ask what, if any, safeguards the seller has in place to ensure that the vendor complies with its contractual obligations. Is there a vendor management plan or audit process in place? Do vendors self-certify? Are vendors required to provide evidence of minimum cybersecurity insurance coverage, and does that coverage extend to the seller? Are there clearly defined indemnification obligations governing which party will bear the economic risk in the event of a data breach and, if so, is the party that bears the indemnification obligation financially capable of satisfying those obligations? A review of

*Continued on page 4*

 *Continued from page 3*

the seller's insurance policies should include a focus on cybersecurity coverage, coverage limits, exclusions, and notification requirements that may impact the seller's ability to recover under an insurance policy if it does not strictly adhere to such requirements.

## Addressing and Mitigating Cyber Risk

Once thorough cyber diligence is conducted, the parties to an M&A transaction can take measures to mitigate, as much as possible, the risk and potential exposure for any issues that have been identified.

The seller and buyer should work together to correct flaws in cybersecurity in advance of closing, if possible, including IT systems updates, as well as updates to company policies and programs. To the extent full corrective measures are not possible pre-closing, the parties should implement a post-closing plan to further strengthen security and ensure effective systems integration, with milestone targets at 30, 60, and 90 days post-closing.

With respect to any known cyber risks that were identified in the diligence process, the parties should negotiate specific protections within the definitive agreement for the transaction. At a minimum, from the buyer's perspective, this should include fulsome representations and warranties from the seller around cybersecurity issues, including:

- ☑ Representations as to the seller's compliance with cybersecurity industry standards and disclosure of all applicable regulatory or contract requirements relating to cybersecurity and data protection;
- ☑ Representations as to the seller's compliance with any applicable reporting requirements; and
- ☑ Disclosure schedules detailing all known prior or existing breaches.

The buyer may wish to negotiate for longer survival periods for cybersecurity representations in the definitive agreement given the long potential latency of claims related to a breach. In addition, for any known breaches or known cyber vulnerabilities, the buyer may desire special indemnification rights, including carving out claims arising from those matters from any applicable indemnification cap or other indemnification limitations. The buyer may also wish to require an increased or lengthier escrow of purchase price funds to cover any such claims. Ultimately, depending on the severity of any issues identified in diligence, the buyer may need to seek a downward adjustment to the purchase price due to an overall decrease in the target's enterprise value.

It is never possible to know the full scope of risk in any M&A deal, and cybersecurity risks can be particularly difficult to identify and quantify, but failure to address cybersecurity risks can lead to potentially catastrophic losses on both sides of the table. It is in both parties' best interest to work from the outset of the diligence process to understand these issues in order to provide the time and opportunity to mitigate them as much as possible in advance of closing and avoid messy and prolonged post-closing disputes.

**About the Authors:** Kathryn Hickey is a partner and chairs the Business and Corporate Group. She may be reached at khickey@pilieromazza.com. Dave Shafer is an associate in the Business and Corporate Group. He may be reached at dshafer@pilieromazza.com.

# Hackers Are No Match for Employee Missteps

By Nichole Atallah and Tony Batt

Do your employees understand how they might be exposing the company to risk simply by working remotely, losing documents, or failing to properly discard information? Imagine John Doe has access to company files and emails on both his laptop and cell phone. One day, John stops by a local coffee shop and logs into its free, public wi-fi on both his work phone and his laptop. Just as John starts sipping his coffee and checking his work email, he unknowingly becomes a victim of a hacker. Because of John's carelessness, this hacker now has access to all of the company's proprietary data and sensitive client information that John could access.

In an age where large companies, such as Target Stores, Sony, Marriott, and Yahoo!, have all scrambled to address data breaches, the external forces and highly technical defenses that are at issue often garner the most attention. However, poor data security culture and policy breakdowns can lead to data security vulnerabilities that are equally, if not more, damaging. In a 2018 survey of business owners by Shred-It, an information security company, 47 percent of business owners reported that

*Continued on page 5*

employee negligence relating to documents or internet use had caused a data breach within their organizations.

Whether you are just turning toward cultivating a work environment that emphasizes data security or have been focused on this issue for years, below are five recommendations any company should consider implementing as front line defenses against a data breach.

## TIP 1 Create a Culture That Values Protecting Information

The value employees place on protecting company information starts at the top. It is important to evaluate how your organization can emphasize the critical role employees play in protecting information and how seriously the company takes violations of company data security policies. Creating this culture necessitates a review of internal policies, but efforts cannot stop there. Management teams need to ensure that those policies and best practices are communicated clearly and frequently.

**"In a 2018 survey of business owners by Shred-It, an information security company, 47 percent of business owners reported that employee negligence relating to documents or internet use had caused a data breach within their organizations."**

## TIP 2 Evaluate Internal Data Protection Controls

In light of evolving requirements for government contractors and new laws that govern data protections at the state level, it is important to ensure that your internal data security protections are up to current standards. For example, your company should have a process for regularly updating anti-virus and malware protections and ensuring proper password protection. Passwords should be sufficiently complex and not duplicative of any passwords an employee has previously used for any other website or application. In addition to information technology controls, there are often documents with sensitive information in print that need to be protected. It is important to have processes for locking up sensitive data, properly discarding of documents no longer in use, and taking print data out of the office.

## TIP 3 Consider Additional Protections for Remote Work

Although the best protection against data vulnerability due to using untrusted networks is to completely abstain from using them, this option is not practical for many businesses. Employers can reduce the risk of a security incident by requiring employees to use a mobile hot spot or a cellular tether to access information in remote, unsecure locations, or providing employees with a Virtual Private Network (VPN) to encrypt traffic over the internet. Also, for employers that allow employees to use their own cell phones and/or laptops to access work material, it is essential to have a clearly established Bring Your Own Device (BYOD) policy that includes a requirement for employees to maintain passwords on those devices as well as pre-approved anti-virus and malware protection.

## TIP 4 Do Not Get Overwhelmed

Data security compliance and risk can be overwhelming to companies that already have a lot on their plates and are concerned about managing the process and related costs. Rest assured, there are ways to manage cost and resources, while also taking into consideration reasonable, business conscious measures. Additionally, there are increasingly more federal and state programs that provide financial assistance to help companies minimize data security risks.

## TIP 5 Ask for Outside Help

There are a number of consultants that provide services to companies of all sizes to assess system vulnerabilities. Moreover, legal counsel can assist in ensuring your policies and practices meet the applicable legal standards. In the event of a data breach, it is important to seek assistance to understand the scope of potential legal liability and to mitigate these risks as quickly as possible.

**About the Authors:** Nichole Atallah is a partner and heads the Labor & Employment Law Group. She may be reached at natallah@pilieromazza.com. Tony Batt is an associate in the Litigation, Labor and Employment Law, and Business and Corporate Groups. He may be reached at abatt@pilieromazza.com.

For any questions or concerns about this issue, or to submit a guest article, please contact our editor, Michelle Litteken, at mlitteken@pilieromazza.com or 202-857-1000.

## When Hackers Attack: Disclosure Obligations and Litigation Risks When You Suffer a Data Breach

By Matthew Feinberg and Emily Rouleau

We are all familiar with the headlines: "Data Breach at Trusted Company Compromises Millions of Users' Personally Identifiable Information." Over the past few years, high-profile companies such as Marriott, Yahoo!, and Target Stores notified consumers that they suffered a data breach, exposing millions of customers' private information. There were nearly 1,500 reported data breaches in 2017 alone, affecting companies of all sizes over a wide range of industries. And, government contractors are not immune from the risk. So, what must you do and what must you be ready for when you have detected a data breach at your company?

There is no blanket federal law pertaining to data privacy and breach notifications for government contractors. But, that does not necessarily mean a government contractor has no duty to report a data breach. For instance, industry-specific laws may impose disclosure requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), which applies to contractors working with healthcare and health records. Individual agencies may also impose reporting requirements. In fact, in January 2017, the Office of Management and Budget (OMB) set minimum requirements for federal agencies to follow when responding to cyber breaches. And, agencies incorporate their own policies into awarded contracts. The DoD, for instance, requires contractors, by regulation, to report cyber incidents. And, the GSA is expected to formalize similar rulemaking over the next few months after relying on OMB's memorandum. Outside these requirements, government contracts may impose particularized data privacy and breach disclosure requirements as well, which may then flow down to subcontracts.

Currently, all 50 states maintain data breach laws. These statutes typically explain who must comply with the law, the types of information that must be protected, the type of data breach that requires notification, and the specific notification requirements that will apply. Some statutes also impose penalties or allow affected parties, or the state itself, to file lawsuits. Although the general concepts are the same, each state statute treats confidential information and data breaches somewhat differently.

In Virginia, for example, if unencrypted and unredacted personal information is accessed by an unauthorized person, whoever owns or licenses the personal information must disclose the breach to the Office of the Attorney General and any affected Virginia resident without unreasonable delay. If a breach affects the personal information of more than 1,000 people, the company also must notify consumer reporting agencies of the timing, distribution, and content of the notice. Notably, the Virginia statute provides the possibility for a lawsuit brought by the Commonwealth and potential civil fines of up to $150,000 per breach.

**"Compliance with agency regulations and contract requirements is particularly critical for government contractors, because the failure to make adequate disclosures of the data breach can result in potential liability under the False Claims Act."**

Similarly, Maryland's Personal Information Protection Act requires businesses that own or license a resident's personal information to maintain reasonable security procedures. When a business discovers a breach, it must conduct a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If, after investigating, the business determines that the breach created a likelihood that personal information has been or will be misused, it must notify individuals as soon as reasonably practicable, but not later than 45 days after conclusion of the investigation. If the company determines that notification is not required, it must record its determination and keep the record for three years. The business must also notify, without unreasonable delay, the Office of the Attorney General and, if more than 1,000 individuals must be notified, each consumer reporting agency. Violations of Maryland's law are considered unfair or deceptive trade practices, and individuals can bring an action to recover for injury or loss sustained.

For these reasons, the first step a company must take when facing a data breach is to engage knowledgeable

*Continued on page 7*

counsel to guide the company through crisis management and internal investigation, assist with loss mitigation, ensure compliance with state laws, agency regulations, as well as prime and subcontract provisions, and make all required disclosures to the right parties at the right times. Compliance with agency regulations and contract requirements is particularly critical for government contractors, because the failure to make adequate disclosures of the data breach can result in potential liability under the False Claims Act. Contractors should also be ready to defend against a possible civil lawsuit from a state government or a class action from one or more affected parties.

Ultimately, a contractor will be best equipped to handle a data breach when it implements robust data privacy and security policies, understands the cybersecurity laws that apply to it, and maintains a relationship with a trusted legal advisor who can guide the company through the complex requirements of state laws, agency regulations, and federal contracts.

**About the Authors:** Matthew Feinberg is an associate in the Litigation, Labor and Employment Law, and Business and Corporate Groups. He may be reached at mfeinberg@pilieromazza.com. Emily Rouleau is an associate in the Government Contracts, Business and Corporate, Litigation, and Labor and Employment Law Groups. She may be reached at erouleau@pilieromazza.com.



## Data Breaches and Data Rights: How the Rights of You and Your Customers Are Impacted

By Cy Alba

Data is ubiquitous. This means that the risk of theft, or simple loss, continues to increase as more information is stored in less secure and decentralized systems. While what we see in the news is usually focused on intrusions that reveal consumer/user information (such as personally identifiable information (PII), personal health information (PHA) under HIPAA, passwords, or similar data) the risk of intellectual property (IP) loss could be even more problematic and costly. This is especially true if you are using third party IP to perform work. In such cases, a breach likely means not only an embarrassing situation, but also a breach of license agreements and/or non-disclosure agreements that could cause you to lose the ability to access the IP entirely and expose you to liability for the loss. If that IP is critical to contract performance, you then risk termination for cause, financial penalties, and poor past performance assessments. These consequential losses can last for years.

If, by example, a prime contractor is using third party code via a traditional license agreement, and uses that code to build software for government use, there are a few issues that could arise. The first concerns ownership and licensing. For that reason, the prime and subcontractor need to understand the ownership and license requirements in the FAR/DFARS. For example, if the prime contractor is using commercial software developed at 100% subcontractor expense prior to performance, and the prime contractor has a license agreement with the subcontractor, the prime contractor should ensure that the license agreement terms are passed to the government. If the terms were not passed on to the government, the prime contractor may be in breach. Notably, it is possible for a prime contractor to constructively promise the government unlimited rights in data or software without having the rights from the subcontractor. In the example above, if the prime contractor did not pass on the license terms, the government's default position is that it takes unlimited rights in all software delivered, or even developed but not delivered, in performance of the contract. In the case where a prime contractor does not have such

*Continued on page 8*

rights, the prime contractor breaches its contract with the government, but also its license agreement (most likely) with the subcontractor that provided the code. The prime contractor is then in a position of possible double liability, especially if the government shares the information with another contractor, acting under the assumption that it has unlimited rights. While this situation is similar to a data breach caused by hacking, what distinguishes it is that it was completely within the prime contractor's control and should have been prevented.

**"If the prime contractor has no idea who took the information or where it is, the attempts at clean up can cost an infinite amount of money and resources, and it will be impossible to effectively determine the scope of the breach or the efficacy of the clean-up performed."**

Second, and more directly to the point, a prime contractor can run into the same type of liability if it fails to follow the cybersecurity requirements in the contract. As noted, you will certainly be in breach of contract if you are hacked and you failed to follow the express requirements. There are additional cybersecurity requirements contractors should be aware of. For example, the contract may reference agency policies. In those cases, depending on the language of the contract, a failure to follow that guidance may also be a breach. Adding third parties only adds complexity. If you have no idea who actually hacked your systems or where that data resides, then it can be nearly impossible to stop its spread or even identify the scope of the leak and its impacts. If you signed a license agreement with a software company, as in the example discussed above, the software company may assume that the IP has been delivered to competitors, or hostile countries who may try and either use the code to develop its own competitor, sell the information to others, or use it to compromise government systems. All of that will cause large losses for the subcontractor, and it will certainly hold the prime responsible for the breach.

Additionally, the software license agreements may also have provisions providing for liquidated damages or presumed damages. In these cases, the prime contractor may have to expend significant funds to mitigate the leak, but also be on the hook for specific dollar amounts for each day the leaked information is not retrieved and such retrieval verified. Such verification may be impossible, in which case the subcontractor may attempt to recover much more than the value of the data/software itself. Courts certainly act in such cases and often refuse to allow such massive recoveries, but only after briefing on the case and, in some cases, costly discovery. Thus, as with all things, a penny of prevention is worth a pound of cure (or many pounds in this case).

Lastly, if the data was classified, there are a host of other concerns. First and foremost, there could be criminal violations, but, even putting that aside, the DoD's rules for spillage of classified information can make the contractor liable for clean-up. If the prime contractor has no idea who took the information or where it is, the attempts at clean-up can cost an infinite amount of money and resources, and it will be impossible to effectively determine the scope of the breach or the efficacy of the clean-up performed. Once that information is out on the internet, it is nearly impossible to track down and eliminate. As such, the government will likely undertake extensive measures, and it may charge the contractor for such attempts. Just one such incident can bankrupt even the largest company, much less small to mid-sized firms working on tight budgets. It should also be mentioned that while insurance can help cover perhaps $1M in losses, perhaps a few million, depending on the policy, the consequential damages are sometimes exempted from coverage or, even if covered, would not come close to the amounts necessary. For these reasons, on classified contracts, it is imperative that you have a robust system that meets all contractual requirements and other standards.

In sum, a data breach is not just about leakage of sensitive information, but may also be much more serious and more difficult to address. If you are working with highly proprietary IP from vendors and subcontractors (or the government itself), such a leak can bankrupt a company, result in litigation, or provide the basis for poor past performance reviews. For these reasons, it is critical that companies understand their cybersecurity requirements and those imposed on them by license agreements and subcontracts so that they are not taken by surprise if an incident happens, and so they have solid defenses against claims by licensors or the government.

**About the Author:** Cy Alba is a partner and is a member of the Government Contracts and Small Business Programs Groups. He may be reached at ialba@pilieromazza.com.