SUFFOLK COUNTY
WOMEN'S BAR ASSOCIATION
of the STATE OF NEW YORK

THE PRESIDENTS MESSAGE

As I write this, the 2016 presidential election has concluded. While the campaign was certainly divisive, as it does every four years, the country now moves on to the business of governing. Whatever your political leanings, it was still a thrill to see a woman's name on the ballot for the highest office in this land. My hope is that one day, we will have the opportunity to cheer a woman as she takes the oath of office and gives the inaugural address prior to taking up her post as president of this great country.

My thanks to Kathy Small, Robin Abramowitz and Margery Weinroth for their efforts in support of WBASNY's voter registration drive. As you have seen from WBASNY President Jaci Flug's communications, the Women's Bar Association of the State of New York exceeded its goals for new state-wide voter registrations. Voting is our most basic privilege as citizens, and I think we can all agree that it is never to be taken for granted.

The SCWBA has been busy, thanks to our VP of Programs Megan Tomlin and our networking luncheon coordinator Lisa Bisagni-Johnson's efforts in putting on interesting and informative programs for our members. Our membership cocktail party in September at the Watermill was not only well-attended, but brought us almost halfway to our goal for membership applications and renewals for this year. At our October program at the Irish Coffee Pub, Hon. Karen Wilutis and Hon. George Harkin gave us an informative analysis of the current issues concerning domestic violence from their perspectives on the District Court and Family Court benches, respectively. In furtherance of October's breast cancer awareness objectives, the SCWBA also took part in a JALBCA (Judges and Lawyers Breast Cancer Alert) Alert on September 28th, in conjunction with the Women in the Courts Committee headed by past President Hon. Isabel Buse, by passing out informational pamphlets and advertising the free mammogram van provided by JALBCA on October 7th. Past President Janessa Trotto has been organizing these events for several years and took an active part in the Alert and in coordinating the "scan van" with JALBCA.

At our east end meeting at the Cooperage Inn in Baiting Hollow, Suffolk County Surrogate John M. Czygier, Jr. gave an informative, as well as entertaining CLE program on the unintended consequences of failing to update one's will after a major life event, in this case, divorce. In addition, our October and November networking lunches explored the topics of domestic violence and breast cancer detection. I hope you will be joining us at our Holiday Party on December 15th at the Bonwit Inn in Commack, where we will have a convivial celebration, as well as a raffle supporting the work of Habitat for Humanity. Items being offered in our raffle will include several, varied gift baskets and a weekend at a Montauk coop generously donated by past President Val Manzo. We are also offering an incentive to those members who renew or join by December 15th: a free CLE program. The drawing will take place at the Holiday Party. So, if you have not renewed, or know of anyone else who may be on the fence about joining, please consider doing so at this time

to take advantage of this incentive, as well as all the other benefits that membership in the SCWBA offers. For future events/programs, please consult out website (suffolkwomensbar.org) and click on the calendar tab.

As a chapter of the Women's Bar Association of the State of New York, we provide delegates to WBASNY and take part in state-wide initiatives, including commenting and voting on proposed legislation affecting women and children. Our voice as part of the larger organization, which is currently on track to break all membership records, can have a significant impact. If you have not done so, I urge you to attend a WBASNY Board meeting. While each chapter only has one vote in the many committees meeting that day, the substantive committees are open to all members. The next quarterly meeting will be on Saturday, January 28, 2017 and will take place at the New York Life Insurance Company in New York City. Of course, also keep in mind our annual Convention, which will be held in May, 2017 at the Water's Edge resort and spa in Westbrook, Connecticut. We are currently accepting proposals for CLE programs at the Convention. Please consult the WBASNY website (www.wbasny.org) for further information on this and other items of interest, including a new member benefit concerning 529 college savings plans.

In the meantime, I wish you all a happy and healthy holiday season, and the time to enjoy being with family and friends.

CORRESPONDING SECRETARY MESSAGE

This is our second quarterly newsletter and you will find that we have included articles about confidentiality and cyber issues. Whether you accept that the election results were in any way affected by Russian hackers, it is clear that lack of cyber security during the presidential campaign led to the mass dissemination of emails that the authors would rather never became public. Cyber-security and data privacy are hot issues and will be getting hotter as state and federal agencies and legislators promulgate new laws and regulations to ensure that data is protected and which seek to impose increasing duties on parties who hold or transmit private data of their customers or clients. We hope that you find these articles interesting and useful in your practices.

On December 15, 2016, we celebrated the holidays at our annual Holiday Party at the Bonwit Inn. For a change of pace, the party was held on the first floor by the bar which allowed our colleges from the matrimonial bar to mix and mingle and participate in our Chinese auction to benefit Habitat for Humanity. In fact, we raised just over $600 for this worthy cause. There were some great prizes auctioned off including a weekend at Val Manzo's co-op in Montauk, as well as baskets filled with wine, soaps and lotions, gourmet olive oil and balsamic vinegar, and chocolates to name a few. I was lucky enough to win the Crushed Olive basket and my table mate won the scratch off lottery wreath. Good luck to her! We all congratulated Megan Tomlin who was nominated for WBASNY's New Lawyer Award, and Margery Weinroth who was nominated for the Marilyn Menge award. The food was good and the company was excellent. A good time was had by all.

Congratulations are also due to our members Hon. Toni A. Bean (District Court), Kathy G. Bergmann (Family Court) and Hon. Martha Luft (Family Court) in their respective judicial races. We are so proud of all of you!

If you have any area of interest that you want to read about in the newsletter, please let me know and we would be happy to reach out to attorneys willing to write about those topics. Better still, I would like to showcase you,

our members, in articles written by you about your area of practice or things that are of interest to you. Linda Morrone, our President, said it best when she said that the SCWBA is your bar association. What better way to make it yours than to submit an article written by you to showcase your talents and expertise. I welcome all submissions, but please be sure to have your articles in to me no later than March 1, 2017 for our next publication date which I expect will be April 1, 2017. To submit articles, please email me Leora Ardizzone, at lardizzone@rmfpc.com or call at 516-663-6538.

UPCOMING EVENTS

Please log onto www.suffolkwomensbar.org or check your mail and email for upcoming events. Notably, our next networking lunch will be on January 11, 2017 at Shandon Court. It is bring a friend day for that lunch as we continue to make efforts to increase membership in the SCWBA. Please remember to join us for lunch and bring a friend who you think would be interested in joining our organization. Mark your calendars for January 24, 2017 for our program "Representing a Client in Arbitration" to be held at the Suffolk County Bar Association. Our own Lisa Pomerantz and Robin Abramowitz will be presenting. Please make every effort to attend. February 8 is our following networking lunch and on February 28 we have a very special "Special interest Bar Association Mixer" to be held at Touro Law Center. We look forward to seeing everyone at these events and the ones scheduled for March and beyond.

IMPORTANT NOTICE

NOTICE OF ELECTION OF NOMINATING COMMITTEE

PLEASE TAKE NOTICE that at the January meeting there will be an election of members to the Nominating Committee.

Nominations shall be made from the floor at the January meeting. Only members in good standing may make a nomination. The consent of the nominee shall be obtained from the member making the nomination, and no person who is absent from the January meeting shall be nominated unless her or his consent has previously been obtained in writing. If more than three (3) persons are nominated, voting shall be done by ballot and the three (3) persons receiving the largest number of votes shall be declared elected.
Only those in attendance and eligible to do so may vote at the January meeting. There must be a quorum of at least 25 members for the election to take place. Please make every effort to attend the January meeting.

Date: January 24, 2017
Time: 6 pm
Location:
Suffolk County Bar Association
560 Wheeler Road
Hauppauge, NY

CAN YOU KEEP A SECRET?... MAINTAINING CONFIDENTIALITY WHILE SELLING YOUR BUSINESS

Selling a business can be an emotionally trying time, fraught with demons both real and imagined. Near the top of the nightmare list is the fear that information about an impending sale will be leaked prematurely to employees and business partners, jeopardizing long-standing relationships and causing defections that can both kill a deal and seriously damage the business itself. Of equal concern to business owners is the risk that critical information shared with potential buyers during the due diligence process will be used for competitive advantage if the transaction fails to close.

While a well drafted confidentiality agreement can be effective in maintaining the confidentiality of a proposed sale, there are a number of steps that business owners can take to reduce the likelihood of an inadvertent disclosure. First, buyers should be pre-screened so as to limit the number of suitors to those most likely to make a serious offer. Using an investment bank or business broker can greatly assist in qualifying potential buyers while reducing dependence on employees in the due diligence and negotiation process. Second, to the extent that non-management employees are needed to facilitate the sale, their loyalty and discretion can be significantly enhanced by appropriate compensation arrangements that help allay their concerns about the future while aligning their interests with those of the business owners. Finally, because many buyers including public companies and private equity funds typically require that the companies they buy have audited financial statements, forward-thinking owners will start having their financial statements audited well before the first buyer walks through the door. This will help facilitate a sale without raising questions among employees who might otherwise suddenly witness a number of unfamiliar faces appearing at the company poring through the company's books and records for no obvious reason.

While a seller may succeed for a time in keeping knowledge of the sale private, sooner or later, employees, customers and suppliers will need to be notified. A wide variety of factors will influence the timing of the disclosure, including whether the buyer insists on contacting key employees, customers and suppliers as part of its due diligence investigation, the existence of anti-assignment or change of control provisions in significant contracts, the need to negotiate with other third-party constituencies, (e.g., unions and lenders), the extent of sale rumors in the company and the industry, and whether and when federal securities laws will require the buyer to publicly disclose the transaction.

From a seller's prospective, the goal is almost always to delay the disclosure until the buyer is "locked in" with a binding contract. But a cautious buyer that has not been given the opportunity to contact key employees, customers and suppliers before the contract is signed may condition its obligation to close the acquisition on its ability to retain these relationships after the closing for its own benefit. The issue of who bears the risk of lost relationships after the deal is announced is often hotly negotiated between buyers and sellers.

To protect the confidentiality of proprietary information, information can and should be disclosed in stages with more sensitive information not shared until late in the process. For example, although a buyer may at some point be entitled to know the seller's gross profit margins for specific customers, there may be no reason to disclose the actual names of those customers until the closing.

.

Poorly advised and inexperienced sellers often divulge more information too early in the sale process than is needed.

Sellers, of course, rely most heavily on confidentiality agreements to protect their interests. From a seller's perspective, this agreement should describe confidential information in the broadest possible terms and apply to all information provided in any format – i.e. oral, written, digital or otherwise. Among the issues to be negotiated are the length of time the agreement will remain in effect, whether a buyer must obtain separate confidentiality agreements from its agents and advisors before sharing seller's confidential information, and how to ensure the return or destruction of information when a transaction fails to close.

Unfortunately, sellers trying to economize on legal fees often either accept a buyer's "standard form" or use a form previously used by seller in another context. Sellers without the benefit of experienced M&A counsel risk irreparable harm as proprietary information is lost to those who will use it for their competitive advantage. Such sellers also lose the opportunity of negotiating for less common but sometimes necessary protection – e.g,.restrictions on the suitor's ability to hire seller's employees if the deal does not close. In a recent sale transaction involving direct competitors, we successfully negotiated on behalf of the seller for the inclusion of a "standstill" provision that required the potential buyer to pay seller if, at any time during the negotiations or six months after negotiations terminated, seller lost a key customer to the buyer, whether or not the loss resulted from the misuse of confidential information.

While the sale of a business will always involve challenges and risks, advance planning, careful thought and professional advice can mitigate those associated with confidentiality and prevent a successful business from becoming damaged goods.

This Article was written by
Irvin Brum, Partner at
Ruskin Moscou Faltischek P.C.

MERGERS AND ACQUISITIONS – THE CYBER-MONEY PIT

In the movie, "The Money Pit", starring Tom Hanks and Shelley Long, Tom Hanks' character, Walter, buys a beautiful house "AS IS". Once the home purchase is completed, the house immediately starts to collapse around them causing the characters to spend a fortune to rebuild their dream home. While the decision to buy "AS IS" made for a comedic premise for the movie, in real life, few people would actually buy a house without a title report, or having the house inspected against structural damage, termite infestation, or signs of leaks or water damage. In Mergers & Acquisitions ("M&A"), anacquiror who neglects to include a rigorous cybersecurity assessment as part of its due diligence takes the same risks as someone who buys a house "AS IS". Any party to an M&A transaction knows that legal and financial due diligence is critical at each stage of the transaction, from valuation to negotiation to closing, and with respect to post-closing integration. As recently demonstrated by Yahoo's disclosure of a prior massive data breach while its acquisition by Verizon is pending, due diligence must also include assessing cyber risks. Many companies have little understanding of cyber risks and, thus, gaps exist in the due diligence process. Effective cybersecurity due diligence should uncover undisclosed and ongoing breaches; malicious software; and weak or non-existent cybersecurity and data privacy safeguards and controls.

If any of these things are not discovered during due diligence, the acquiror may incur unforeseen damages. For example, weak security practices at the target company exponentially increase the possibility of pre-existing breaches and infected target company systems spreading through the entire new organization. In addition to significant harm to an acquiror's reputation and business interruption, the acquiring company could also inherit state and federal regulatory actions, as well as being named by consumers in a data breach class action suit or a shareholder derivate action. Although information about a target's cybersecurity deficiencies is usually discoverable, acquiring companies often lack the proper personnel to conduct thorough analyses.

Thus, a trusted and experienced third party team of legal and technical personnel must be retained in order to provide more than a cursory overview. In certain industries that are more heavily regulated, finding for the acquiror, or add costs relating to risk management or remediation. When considering an acquisition, make sure that your M&A due diligence process includes a thorough assessment of cyber risks in order to properly value and structure the deal. This will help to ensure that cyber risks are mitigated throughout the process and post-closing.

This Article was written by
Leora F. Ardizzone & Seth I. Rubin of
Ruskin Moscou Faltischek P.C.

THE FINANCIAL SERVICES INDUSTRY IN NEW YORK IS ABOUT TO BE POUNDED BY PROPOSED NEW CYBERSECURITY REGULATIONS

On September 13, 2016, Governor Cuomo and the New York State Department of Financial Services ("NYDFS") proposed a sweeping new cybersecurity regulation for financial institutions in New York. The proposed regulation attempts to protect consumers from the consequences of a cyber-attack by forcing banks, insurance companies, and other financial institutions regulated or licensed by the New York Department of Financial Services (collectively "Covered Entities") to adopt an extensive set of cybersecurity protections. Perhaps due to Governor Cuomo's desire to set the standard with a "first-in-the-nation" regulation, New York's proposal goes significantly beyond what other regulators require, and if adopted in its present form will place heavy burdens on most Covered Entities. For instance, Covered Entities are mandated to appoint a Chief Information Security Officer, regularly conduct audits and vulnerability assessments, have their board of directors review and approve their cybersecurity policy and assess risks, encrypt certain information, and annually certify compliance to NYDFS.

Comments on the "Cybersecurity Requirements for Financial Services Companies" are due by November 12, 2016 and unless modified, will become a part of 23 N.Y.C.R.R. Pt. 500, effective on January 01, 2017. Covered Entities are required to comply by June 30, 2017 and NYDFS has the authority to impose civil and criminal penalties for noncompliance.

In other words, time is short for a Covered Entity to assess their cybersecurity risks and/or enhance their cybersecurity program. Thus, this

article is designed to discuss the salient points of the proposed regulation and the potential ramifications and increased liability for Covered Entities and their senior officers.

A Chief Information Security Officer Must be Designated- A Covered Entity will be required to designate a qualified individual to act as the Chief Information Security Officer ("CISO"). The CISO will be responsible for overseeing the implementation of a cybersecurity program and policy for the financial institution. In addition to oversight, the CISO will be required to develop a report, at least bi-annually, and present it to the board of directors. The report must: (1) include an assessment of the confidentiality, integrity and availability of the Information System of the institution; (2) detail exceptions to the policy and procedures; (3) identify possible cybersecurity risks; (4) asses the effectiveness of the program; (5) propose steps to remediate any inadequacies; and (6) include a summary of all material Cybersecurity Events that effected the institution during the time period.

Compliance with this requirement can be costly. The average salary for a Chief Information Security officer in the United States is $204,000 and in New York, that salary can rise to $380,000. This requirement creates a short term and long-term cost that is above what many medium to small financial institutions will be able to afford.

There is a second option for Covered Entities. A third party service provider can fulfill this requirement as long as the Covered Entity: (1) retains responsibility for compliance; (2) designates a senior member of the Covered Entity's personnel responsible for oversight of the third-party service provider; and (3) requires the third-party service provider to maintain a cybersecurity program that meets the requirements of the regulation. However, this option comes with its own challenges, as the Covered Entity would still be liable for any breach or lack of oversight by the third-party service provider. While this option may be less costly, the Covered Entity will be giving up control but will remain subject to enforcement action for deficiencies in the work of the third-party service provider.

A Cybersecurity Program Must be Created- Covered Entities will be required to create and implement cybersecurity programs designed to include the following core security objectives:
(1) identify internal and external cyber risks by, at a minimum, identifying the Nonpublic Information stored on the Covered Entity's Information Systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed;
(2) use defensive infrastructure and implement policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
(3) detect Cybersecurity Events, defined as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System;
(4) respond to identified or detected Cybersecurity Events to mitigate negative effects;
(5) promptly recover from Cybersecurity Events and restore normal operations and services; and
(6) fulfill all regulatory reporting obligations.
As part of its cybersecurity program, a Covered Entity will also be required to establish a written cybersecurity policy that covers fourteen different areas: (1) information security; (2) data governance and classification; (3) access controls and identity management; (4) business continuity and disaster recovery planning and resources; (5) capacity and performance planning; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and third-party service provider management; (13) risk assessment; and (14) incident response.

Moreover, the proposed regulation explicitly requires the board of directors and senior management to be

intimately involved with the cybersecurity program. As indicated above, the Board of Directors must review the cybersecurity policy and assess risks with the CISO at least twice annually. Indeed, the chairperson of the board or senior officer must provide a Certification of Compliance with the NYDFS regulation and maintain records that support the certification for at least five years and make the documentation available to NYDFS upon request. This annual compliance requirement opens the door to significant liability for board members and senior officers if the purported compliance is false or inadequate.

Cybersecurity Event Notification to NYDFS- A troubling provision is the mandated requirement for a Covered Entity to notify the NYDFS within seventy-two hours of becoming aware of a Cybersecurity Event reasonably likely to materially affect normal operations of the Covered Entity or when a Cybersecuirty Event involves "the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information." As an initial matter, seventy-two hours is unrealistic. In the vast majority of cybersecurity incidents, it is impossible to ascertain the facts surrounding a Cybersecurity Event (or whether one actually occurred) in such a short time frame given that a legal and technical team must determine the nature and scope of a cybersecurity incident through forensics, data analysis and an assessment of the affected systems. Moreover, Cybersecurity Event is defined broadly and it is unclear what constitutes an unsuccessful attempt. In other words, as it currently stands, a Covered Entity would be required to report an event before it can determine with certainty whether Nonpublic Information was even accessed.

Other Measures- Other measures required to be taken are: (1) the creation of an audit trail, policies for in-house application, and an incident response plan; (2) limitation of access privileges and data retention; (3) risk assessment; (4) employment of cybersecurity personnel; (5) training for all employees; and (6) encryption for Nonpublic Information at rest and in transit.

How Does This Effect You?
The mandatory requirements are vast and will undoubtedly result in a material increase in operational and compliance costs for Covered Entities. Regardless of whether a Covered Entity has an established cybersecurity program, there will be limited time to assess cybersecurity risks and implement the stringent requirements of New York's proposed new regulations. Thus, it is essential that a Covered Entity immediately begin working towards compliance, including involving its board and senior management in assessing cyber-risks and making it part of the company's overall risk management framework.

This Article was written by
John J. Cooney, Partner at
Ruskin Moscou Faltischek P.C.