Cybersecurity Technical, Legal and Ethical Considerations for Attorneys (and their clients) 2023

Nicholas G. Himonidis, J.D., CFE, CCFS, CCFI, CRC
The NGH Group, Inc.

CONTENT OUTLINE

1. **New York State Cybersecurity CLE Requirements for ALL Attorneys as of 2023**
    a. CLE requirements and details
2. **NYS Data Breach Laws, Notification Requirements, and Cyber Insurance**
    a. New York Stop Hacks and Improve Electronic Data Security Act
    b. New York State Department of Financial Services (NYDFS) Cybersecurity Regulation
    c. New York State Information Security Breach and Notification Act
    d. New York State Data Breach Notification Requirements
    e. Cyber Insurance Considerations for Attorneys
3. **Information Security Best Practices for Attorneys**
    a. Understanding Your Ecosystem
    b. Smartphones
    c. Computers
    d. Apps
4. **Information Security Best Practices for Clients**
    a. Shared Devices and Accounts
    b. Password Management
    c. Home Network (Wi-Fi)
    d. Apple iCloud Bleed
    e. Social Media
    f. One-page checklist for Clients
5. **Digital Espionage Considerations in Matrimonial Litigation**
    a. Clandestine Imaging, Spyware, Legitimate Monitoring Software, and Account Hacking
    b. Advising your Client About the Implications of Spying

Section 1 – New York State Cybersecurity Requirements for Attorneys

Technology is advancing and so are data breaches; attorneys must have technical competence as information security is a shared responsibility model. The tools and applications ("apps") available to attorneys are often built with information security best practices in place, however, attorneys have a duty to ensure their accounts and information is secure.

In New York State, the new cybersecurity CLE requirement effective July 1, 2023, for attorneys is known as the CLE Cybersecurity & Privacy Law Requirement. The requirement mandates that all attorneys who practice in New York State must complete at least one (1) accredited CLE credit hour in cybersecurity and privacy law during every two (2) year reporting cycle. Along with Ethics, Diversity & Inclusion – this is the ONLY other mandated topic area for required CLE in New York.

The CLE Cybersecurity & Privacy Law Requirement was implemented in response to the growing threat of cybersecurity breaches and data privacy violations – and that fact that attorneys and law firms have become prime targets for hackers. The requirement aims to ensure that all attorneys in the state have a basic understanding of cybersecurity and privacy law, which will enable them to better protect client information and confidential data.

There is a slight variation in the requirement depending on whether you are an "experienced attorney" or a "newly admitted attorney" and is detailed in the FAQs provided by the state. The Cybersecurity, Privacy and Data Protection category of CLE credit has two (2) parts: Ethics and General. As defined by the state:

Cybersecurity, Privacy and Data Protection-Ethics must relate to lawyers' ethical obligations and professional responsibilities regarding the protection of electronic data and communication and may include, among other things: sources of lawyers' ethical obligations and professional responsibilities and their application to electronic data and communication; protection of confidential, privileged and proprietary client and law office data and communication; client counseling and consent regarding electronic data, communication and storage protection policies, protocols, risks and privacy implications; security issues related to the protection of escrow funds; inadvertent or unauthorized electronic disclosure of confidential information, including through social media, data breaches and cyber-attacks; and supervision of employees, vendors and third parties as it relates to electronic data and communication.

Cybersecurity, Privacy and Data Protection-General must relate to the practice of law and may include, among other things, technological aspects of protecting client and law office electronic data and communication (including sending, receiving and storing electronic information; cybersecurity features of technology used; network, hardware, software and mobile device security; preventing, mitigating, and responding to cybersecurity threats, cyber-attacks and data breaches); vetting and assessing vendors and other third parties relating to policies, protocols and practices on protecting electronic data and communication; applicable laws relating to cybersecurity (including data breach laws) and data privacy; and law office cybersecurity, privacy and data protection policies and protocols.

Section 1 Resources:

Guidance Relating to the New Cybersecurity, Privacy and Data Protection Category of CLE Credit: https://www.nycourts.gov/LegacyPDFS/attorneys/CLE/Cybersecurity-Privacy-and-Data-Protection-Guidance-Document.pdf

Cybersecurity, Privacy and Data Protection FAQs: https://www.nycourts.gov/LegacyPDFS/attorneys/CLE/Cybersecurity-Privacy-and-Data-Protection-FAQs.pdf

17a-Rules-1500-2h-Cybersecurity-Definition.pdf: https://www.nycourts.gov/LegacyPDFS/attorneys/cle/17a-Rules-1500-2h-Cybersecurity-Definition.pdf

17b-Rules-1500-22a-Cybersecurity-Experienced-Attorney-Requirement.pdf: https://www.nycourts.gov/LegacyPDFS/attorneys/cle/17b-Rules-1500-22a-Cybersecurity-Experienced-Attorney-Requirement.pdf

17c-Rules-1500-12a-b-Cybersecurity-Newly-Admitted-Attorney-Requirement.pdf: https://www.nycourts.gov/LegacyPDFS/attorneys/cle/17c-Rules-1500-12a-b-Cybersecurity-Newly-Admitted-Attorney-Requirement.pdf

Section 2 – Data Breach Laws, Reporting Requirements, and Cyber Insurance

With the volume of data breaches increasing, attorneys practicing in New York State should also be aware of specific laws, regulations, related reporting requirements, and cyber insurance as well. Not only will this help attorneys and law firms be prepared should an unfortunate event occur, but knowledge of these laws and regulations, and some general knowledge of the insurance coverages available for these risks, may be relevant to their clients as well.

NYS Data Breach Laws and Regulations

New York State currently has a few data breach laws and regulations that certain attorneys and law firms practicing in the state will fall under including the New York Stop Hacks and Improve Electronic Data Security Act– also known as the SHIELD Act, the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation– also known as 23 NYCRR Part 500, and the New York State Information Security Breach and Notification Act.

The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act is a data security law in NYS that was enacted on July 25, 2019. The SHIELD Act updates and strengthens New York State's data breach notification law and requires certain entities to implement reasonable data security measures to protect the private information of New York residents.

Under the SHIELD Act, entities that own or license private information of New York residents must develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the private information. (This would certainly apply to lawyers / law firms practicing family law as they undoubtedly collect and maintain 'private information' of their clients, and often times of opposing parties – for example – Statements of Net Worth). The Act does not prescribe specific security measures but requires the safeguards to be "appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of the private information." Given the nature of some information collected and maintained by matrimonial attorneys, "appropriate" measures may be interpreted to be fairly significant, even in the case of small firms / solo practitioners.

The SHIELD Act also expands the definition of "private information" to include not only traditional personally identifiable information (PII) such as Social Security numbers and financial account information but also includes biometric information, such as fingerprints and facial recognition data, and email addresses or usernames in combination with passwords or security questions and answers.

Additionally, the SHIELD Act updates New York State's data breach notification law by expanding the definition of a data breach and requiring that notification be made to affected individuals and the New York State Attorney General's Office within a certain timeframe. The Act also imposes certain notification requirements on third-party service providers in the event of a data breach affecting the private information of a covered entity's New York residents.

Overall, the SHIELD Act aims to improve data security practices and protect the private information of New York residents. ***For law firms that collect, maintain, or process private***

information of New York residents, they should review their current data security measures and policies to ensure compliance with the SHIELD Act's requirements. This may include implementing measures such as encryption, access controls, and regular risk assessments, and developing incident response plans and breach notification procedures. Further, law firms must be able to demonstrate they have implemented proper controls.

The New York State Department of Financial Services (NYDFS) Cybersecurity Regulation, 23 NYCRR Part 500, is a set of cybersecurity requirements that apply to all entities regulated by the NYDFS, which includes certain types of law firms that are licensed or authorized to operate in New York State, such as those providing financial or insurance-related legal services. The Regulation applies to Covered Entities, which are defined to include organizations operating under a license or registration under the NY Banking Law, Insurance Law or Financial Services Law. The Regulation separately refers to Authorized Users and Third-Party Service Providers (TPSPs) that are authorized to access or use a Covered Entity's information systems and data. A TPSP will need to comply with the cybersecurity requirements imposed on it by the Covered Entity it serves. The regulation was first proposed in 2016 and became effective on March 1, 2017. Proposed amendments were published on November 9, 2022, and are currently being reviewed.

In addition to the cybersecurity program requirements, the NYDFS Cybersecurity Regulation also requires covered entities to implement several specific cybersecurity measures, including maintaining a written cybersecurity policy, conducting periodic risk assessments and penetration testing, implementing multi-factor authentication, providing regular cybersecurity awareness training, developing an incident response plan, encrypting all non-public information, and maintaining audit trails.

The NYDFS Cybersecurity Regulation also requires covered entities to report cybersecurity events to the NYDFS and to maintain certain records related to cybersecurity events for a period of five (5) years.

Overall, the NYDFS Cybersecurity Regulation is designed to promote the protection of sensitive information and the integrity of the financial services industry in New York State. Covered entities and law firms that are considered TPSPs should ensure compliance with the regulation's requirements to avoid potential legal and reputational consequences.

While the NYDFS Cybersecurity Regulation may not apply to law firms exclusively engaged in matrimonial law – all attorneys should be aware of these regulations.

The NYS Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law. Details regarding notification requirements are in the section below.

New York State Data Breach Notification Requirements

Law firms have an ethical and legal obligation to report cyber breaches that involve the unauthorized access, use, or disclosure of confidential client information or other sensitive data.

In the United States, most states have data breach notification laws that require businesses, including law firms, to report any breaches that involve the unauthorized access or acquisition of sensitive personal information. The notification requirements may vary by state, but typically include factors such as the number of individuals affected, the type of information involved, and the nature of the breach.

The SHIELD Act in New York State requires that affected consumers be notified after discovery of a breach where the security of a computer data system affected the private information of a consumer. The disclosure must be made in the **most expedient time possible**, consistent with the legitimate needs of law enforcement agencies. While the law requires notice to the Office of the New York State Attorney General (OAG), the New York Department of State, and the New York State Police of the timing, content, and distribution of the notices and approximate number of affected persons, submission of a breach form through the OAG's data-breach-reporting portal is sufficient, as the information is automatically sent to the three (3) credit reporting entities including Equifax, Experian, and Transunion. The law does provide exceptions to the notification requirements which are detailed on the OAG's website.

In New York State, the reporting obligations following a cyber breach are set forth in the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation, the NYS Information Security Breach and Notification Act, as well as in other state and federal laws that may apply.

Under the NYDFS Cybersecurity Regulation, which applies to all entities licensed or authorized by the NYDFS, **including certain law firms**, entities must report any cybersecurity events that have a reasonable likelihood of materially affecting the normal operation of the entity or that affect nonpublic information to the NYDFS as promptly as possible, but **no later than 72 hours after becoming aware of the event**.

Additionally, if the breach involves personally identifiable information (PII) of New York residents, the entity must also comply with the New York State breach notification law, which requires the entity to notify affected individuals, the NYDFS, and other regulators as soon as possible, but **no later than 10 days after discovery of the breach**.

The NYDFS Cybersecurity Regulation also requires entities to maintain records related to cybersecurity events for a period of five (5) years, which may be subject to examination by the NYDFS or other regulatory agencies.

The NYS Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law. State entities and persons or businesses conducting business who own or license computerized data which includes private information must disclose any breach of the data to New York residents whose private information was exposed. (***In other words, and specific to this audience, matrimonial attorneys and law firms operating in, and having clients, in NYS***.) Under section 899-aa of the General Business Law, a person or business conducting business must also notify (in addition to the affected NYS residents) three (3) NYS offices: the NYS Attorney General; the NYS Division of State Police; and the Department of State's Division of Consumer Protection.

Furthermore, law firms may also have reporting obligations under other state or federal laws that may apply, such as the New York State Information Security Breach and Notification Act or the Health Insurance Portability and Accountability Act (HIPAA).

Therefore, if a law firm experiences a cyber breach, they should consult with ***legal counsel experienced in handling cyber breach*** to determine their reporting obligations under applicable laws and regulations and take appropriate steps to comply with those obligations.

Additionally, the American Bar Association's (ABA) Model Rules of Professional Conduct provide guidance to attorneys on their ethical obligations regarding data breaches. Model Rule 1.6(c) requires attorneys to make reasonable efforts to prevent the unauthorized disclosure of client information, and to notify clients promptly of any known or suspected data breaches that may involve their confidential information.

In the event of a cyber breach, law firms should promptly investigate the breach, take steps to mitigate any damage or harm caused, and determine whether any notification obligations exist under applicable laws or regulations. They should also consider their ethical obligations to their clients and take appropriate steps to communicate with affected clients, including providing them with information about the breach and any steps being taken to protect their information.

Overall, law firms should be proactive in developing incident response plans and policies to help prevent cyber breaches and ensure they are prepared to respond appropriately in the event of a breach.

Cyber Insurance Considerations for Attorneys

Cyber insurance continues to be a hot topic for all entities, especially law firms. Year-over-year, premiums are skyrocketing as ransomware and business interruption are primary drivers, with an uptick in social engineering and fraudulent payment incidents. Also increasing year-over-year are the number of law firms that have cyber liability insurance, however, according to the ABA, that number is still below 50%.

Law firms should consider several factors when evaluating cyber insurance options (or renewals) to ensure they have adequate coverage in the event of a cyber incident. Below are some key considerations:

1. *Coverage Limits*: The law firm should ensure the insurance policy provides sufficient coverage for potential losses related to a cyber incident, including but not limited to, legal fees, damages, and costs related to data recovery, notification, and forensic investigations.

2. *Specific Coverage*: The law firm should ensure the policy covers specific risks that are relevant to their business, such as social engineering scams or ransomware attacks.

3. *Retroactive Coverage*: The law firm should ensure the policy provides retroactive coverage for any incidents that may have occurred before the policy was purchased, but are not discovered until after the policy is effective, as cyber incidents can occur and remain undetected for months or even years.

4. *Exclusions*: The law firm should carefully review the policy exclusions to understand what types of losses or damages may not be covered under the policy.

5. *Incident Response Plan*: The law firm should ensure the policy provides coverage for incident response planning and execution, including the costs of hiring external consultants or legal counsel to assist with the incident response process.

6. *Third-Party Liability*: The law firm should consider whether the policy provides coverage for third-party liability claims, such as those related to a breach of client or vendor data.

7. *Insurer Reputation*: The law firm should consider the reputation and financial stability of the insurer before purchasing a policy, as well as the insurer's track record of paying claims promptly and fairly.

By carefully considering these factors, law firms can select a cyber insurance policy that meets their specific needs and provides adequate coverage in the event of a cyber incident.

Section 2 Resources:

NY Senate Bill S5575B (SHIELD Act): https://www.nysenate.gov/legislation/bills/2019/S5575

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act): https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

NY OAG Data Breach Reporting: https://ag.ny.gov/resources/organizations/data-breach-reporting

ABA Formal Opinion 483 (Lawyers' Obligations After an Electronic Data Breach or Cyberattack): https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

ABA Formal Opinion 498 (Ethical responsibilities for lawyers when practicing virtually including cybersecurity): https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf

NYSBA Cybersecurity Guide for Attorneys: https://archive.nysba.org/nysbacyber/

NYS Information Security Breach and Notification Act Factsheet for Businesses: https://dos.ny.gov/system/files/documents/2021/09/infosecbreach.pdf

Sample letter from a breaching entity to notify New Yorkers of a Security Breach Incident: https://dos.ny.gov/data-security-breach-notification-sample-letter

Section 3 – Information Security Best Practices for Attorneys

Lawyers generate, send, and receive a great deal of sensitive and legally privileged data. As such, they are legally and ethically responsible for the security of that data. On a more practical level, the 'dataspheres' lawyers operate in today are such that without the direct and meaningful participation ***of every end user*** (every attorney / assistant / paralegal in the firm), the most herculean efforts of the most competent IT people won't be sufficient. Many attorneys don't know where all their sensitive data lives – and perhaps more importantly – do not keep careful track of the myriad of ways they access that data. Most attorneys are too busy with day-to-day case work to give these questions serious thought—and that is a dangerous mistake. Most would probably say their data is stored on a "secure" email server or a "secure" file server or it's "in a secure cloud environment" - or that they have an IT company that "secures" their data. But the formidable cyber security defenses of the big data platforms we use, and the 'network security' that our IT professionals are primarily focused on, are NOT how most data breaches occur today. ***Vulnerabilities in end user devices (frequently personal devices), and compromises of account login credentials are among the most common attack vectors exploited by hackers.***

Attorneys are prime targets for hackers. According to a 2021 ABA survey, 25% of respondents reported that their firms had experienced a data breach at some time. That number increased to 27% in 2022. One recent action by the New York State Attorney General's Office against a New York medical malpractice firm that fell victim to ransomware resulted in a $200,000 penalty and a requirement to implement data security improvements.

Understand Your Data Ecosystem

Securing your data starts with ***knowing where your data is, and all of the ways to access it***. While this concept may seem overly simplistic, many business owners, including attorneys, don't know where their sensitive data resides, much less consider the platforms and services through which it passes daily. We all have smartphones and computers, likely with multiple email accounts on each. Our phones have apps for both work and personal use. We subscribe to services like Zoom, Dropbox, OneDrive, etc. Our smartphones and tablets, not just our office computers, are linked to email servers, file shares, cloud storage systems, databases, and other applications. Nearly every device we use has sensitive data stored on it, passing through it, or is a conduit to access that sensitive data.

Knowing where the sensitive data is stored, and what devices and apps can access that data, is the first, and most critical step to securing that data. Why? Because hackers frequently target the weakest attack vector (or point of entry) – and most often that's YOU – the end user. Why should they break through a solid steel door if they can easily steal the key from someone who is careless with it, and perhaps forgot they even had it. You, the 'end user' must develop good cyber security habits on your smart phone, your home computer, your iPad, etc. – or you will continue to be the 'weak link' in the cyber security battle.

Let's discuss some specific actions you can and should take to help protect your sensitive data.

Smartphones

Lawyers communicate constantly on their phones, by voice, text and email. Many also use messaging apps—Facebook Messenger, Instagram, WhatsApp, WeChat, Snapchat, Telegram, Signal, Viber, etc.—in addition to enterprise messaging platforms, like Slack, Teams or Discord. Then, they have email platforms and services, such as Exchange, Gmail, Yahoo, AOL, ProtonMail, Tutanota and others. Of the many apps on those phones, most use only a few regularly; the rest are completely forgotten, and that is a vulnerability in and of itself because unused apps are not regularly updated – and 'security fixes' don't get applied.

So where do we start? First, secure the phone itself. Make sure you have a secure passcode coupled with screen auto-lock set to a very short period (like 1 minute). Next, consider taking the following steps:

- Review all apps and delete those that are no longer used.
- Configure the operating system and all apps to update automatically.
- Review the privacy settings for all apps, especially those with which you share your location, contacts, photos, camera or microphone.
- For apps with access to sensitive data, enable an app-specific PIN code (different from your phone passcode) or use biometrics, such as a fingerprint or facial recognition, to access the app, if available.
- Enable the ability to remotely lock, locate or wipe the device if it is lost or stolen.
- Contact your cell carrier to place extra security on your account, such as requiring a passcode for authorized users to make changes, which will protect against increasingly common SIM swapping attacks to bypass SMS based 2FA.
- Never connect to unsecured / public wireless networks – if absolutely essential – be sure to use a mobile device VPN (Virtual Private Network) app such to secure your traffic on the network;
- Never connect your device to a 'free public charger' such as those found in airports – the FBI recently issued a warning about hackers deploying malware through these devices

Company-issued cell phones are likely being managed by a law firm's IT group, using a mobile device management (MDM) platform that enforces policies in line with industry best practices – but the vast majority of attorneys 'BYOD' – bring their own device – and must therefore accept responsibility for the security posture of that device.

iPhone users need to ***understand how iCloud works*** and take steps to avoid inadvertent "spillover" of iCloud data to any device not used and accessible exclusively by you. The data in your iCloud can sync to any Apple devices with the same Apple ID. Never enter your Apple ID and password into any Apple device that is not used exclusively by you – as your sensitive information may be synced to those devices. You should routinely review the list of devices connected to your Apple ID – and immediately 'log out' any device you are not 100% is yours and can be accounted for. This guidance is also very relevant to clients involved in family and matrimonial matters.

Apple has released a new feature called "Lockdown Mode" in iOS (16) – which, when enabled, provides extremely high protection against digital threats. Attorneys who deal with particularly sensitive data, or routinely access client data from their iPhone may wish to consider engaging this extreme threat protection.

Computers

If you have a firm-issued laptop, it is likely managed through enterprise software that enforces security policies, similar to a firm-issued phone. However, if your laptop (or home desktop used for work) is not being managed this way, be sure to follow the guidelines outlined above for smartphones (as it translates to computers as well), and take these additional steps:

- **Enable full-disk encryption—*especially on laptops*.** This protects anyone, including sophisticated thieves, from copying data directly from the computer's hard drive if it is lost or stolen. This is NOT the same as having a 'login password' – which is easily defeated by professionals. Windows and Mac both have built-in, whole-disk encryption, BitLocker on Windows and FileVault on Mac, but they need to be enabled.
- **Activate a premium antivirus subscription** to provide real-time protection against threats from email attachments or web surfing. Many people with personal computers either received a trial subscription to an antivirus program or downloaded a free version at some point; free and expired trial versions don't carry the same benefits as a premium program, such as real-time scanning, browser scanning, automatic scans, or automatic updates.

While your cell phone temporarily retrieves files stored elsewhere, computers operate differently, and actual copies of files viewed from a remote source often end up cached on the hard drive—another compelling reason to enable full disk encryption, should the computer be lost or stolen.

You need to understand what information is stored on your computer ***and where else it might exist***. Most people are familiar with Desktop, Documents and Downloads folders, but what about email? Let's say you use Microsoft Outlook. All the emails you read and search through have a local copy saved on that computer (and any other computers where you have Microsoft Outlook installed), ***including attachments***. That information also lives on the Microsoft Exchange server and the file server where Exchange is backed up. Even if you only access email from Microsoft Outlook using a web browser (formerly Outlook Web Access, or OWA), any attachments you open are stored on your computer as a cached file. Beyond email, other documents and files are saved in various locations on your computer. If you use Microsoft 365, for example, all that information syncs to Microsoft's cloud and is accessible wherever you log into Microsoft 365.

Much of the sensitive information you generate and receive—through email, shared drives or local apps—exists in many locations, and you must consider how to protect ***every one*** of these potential

"attack surfaces." Do not ever save login credentials for anything of importance in Outlook contacts or notes.

Apps

Apps (on your phone or computer) make accessing all kinds of information easy and convenient, but that convenience comes at the cost of reduced security. Every app has potential vulnerabilities, and lesser-known apps from smaller developers often have far less built-in security, with updates that may be infrequent or non-existent. All apps must be properly configured for security and privacy, and all non-essential or rarely used apps should be deleted. Additional considerations are laid out below.

Accounts for Apps

When signing up for a new app, use your work email for a business-related app and a personal email for a personal app. Be extremely cautious about apps and accounts that offer the option to sign in with another account, such as Google or Facebook. Using this option relies on those other services to secure your login information. If one of those platforms does suffer a breach, and your credentials are compromised, whatever other accounts you signed into this way may also be compromised. Instead, create separate, distinct login credentials for each and every account you utilize (see below regarding the use of a 'password manager').

Passwords for Apps

To generate and keep track of unique, complex passwords for all of your many accounts, consider a password manager such as RoboForm, LastPass, Dashlane, 1Password and others. These utilities offer the ability to automatically generate different, complex passwords for all of your accounts and store them in an encrypted vault. Even though password manager companies are a prime target for hackers, they are still very secure, and using them to store unique, complex passwords for all of your separate accounts is much safer than most of the alternatives. You just have to make sure that the 'master password' you use for your password manager is long, easily memorable to you but not 'guessable' by anyone else, and is one that you have never used before. Commit that one master password to memory, and if absolutely necessary, write it down and store it one very secure place (like a safe).

Multi-Factor Authentication (MFA)

Also referred to as two-factor authentication (2FA) or two-step verification, MFA should never be ignored. Along with good password discipline – it is the single best defense against one of your accounts or 'gateways' to your sensitive data being compromised. Nearly all apps and services offer MFA, and if they don't, you should consider an alternative. Many apps and services offer multiple forms of MFA including SMS (text) codes sent to your cell phone, authenticator apps like Google Authenticator, biometrics, and physical hardware. SMS codes being texted to your phone is the weakest method of MFA - as this can be defeated by SIM swap attacks, which are becoming increasingly common, where a hacker tricks your carrier into porting your phone number to a phone in the hacker's possession – at which point they, not you, will receive the MFA code(s) via SMS.

Wherever possible, use an authentication app, such as Google Authenticator, Microsoft Authenticator or Duo. These are not 'SMS' based, and if you do become a victim of a 'SIM' swap – the hacker will not see the necessary MFA codes – but you still will have access to them.

Remote Access Apps

While the ability to access files or a computer remotely increases productivity and efficiency, it also increases risk. If using a remote-access application, such as TeamViewer, AnyDesk, Splashtop or RDP, ***ensure that your credentials are not saved for automatic access, and enable authenticator app-based MFA***.

File Storage Apps

Apps and services such as OneDrive, Dropbox, ShareFile, Box, and others make it very convenient to access files anywhere, anytime, from any device. This same convenience also makes it easier for hackers to steal files. The devices used to access these apps must have proper security settings enabled, and the apps themselves need to be secured using ***proper password controls and MFA***.

Section 4 – Information Security Best Practices for Clients

When we engage a client in a family law or matrimonial matter, emotions are generally high and there is often significant contention between the parties. For some clients, they are completely unaware of what their estranged spouse or family member may still have access to as it relates to everything digital in their life, or worse yet, what their estranged spouse may do in an attempt to get access to that valuable information. As attorneys, not only are we responsible for protecting the sensitive information we hold, but we also have an ethical obligation to advise our clients to do the same. In addition to the aforementioned best practices laid out for lawyers, below are some key areas where there is an increased risk of our client's information being exposed in matrimonial and family law cases, and how they should be advised to protect it.

Shared Devices and Accounts

Oftentimes family members and spouses share devices or have access to all the devices in a household. The first step for your clients to protect their sensitive information is to know all the devices in the household, if your client has information on them, and who has access to them, whether it is physical access, account access, or both. For any shared devices that are not your client's primary devices, they should remove their information- whether that means deleting files, removing apps, or removing accounts- and refrain from using those devices to access their information going forward. In practical terms for example, advise your client not to access their email from the family room computer. For any primary devices used by your client such as their phone, tablet, or laptop, they should remove any other family members access to those devices. If a device must be shared, such as allowing a child to use a laptop to access schoolwork, they should have a separate account created on that devices that is NOT AN "ADMIN" ACCOUNT and limits their access to only their information and does not expose access to your client's information. The same goes for any accounts or apps; dedicated accounts should be created for those family members

that need access. If your client shares access with an estranged family member to an account or app, they should refrain from using it, remove (or transfer) their account, and create a separate account so there is no overlap of information. This is especially important for highly consequential accounts such as banking, finance, and cell phone service.

Password Management

Once devices have been identified and information or accounts removed, there is an inherent need to create new accounts with new passwords. There is a strong likelihood that many historical accounts have passwords that are either known or could be easily guessed by the estranged family member. For this reason, it is paramount that your clients immediately change their passwords to all accounts starting with the most consequential, and it is highly recommended they consider using a password manager for the benefit of generating unique, complex passwords that can all be secured in a single vault. Again, of course, this vault must be secured with a password that only your client knows and can commit to memory.

When our clients change passwords to existing accounts, they should also conduct a review of other account settings such as recovery phone numbers, recovery email addresses, notification email addresses, security questions, and other privacy/security settings that can be changed to ensure their estranged family members do not have the ability to "recover" access to an account or receive notifications related to those accounts.

Clients must also be reminded that MFA is critical and must be enabled for each account as well. For some clients, this will be nothing new but for others there may be an uncomfortable, but necessary, change to user behavior.

Home Network (Wi-Fi)

All of our clients have different living arrangements; some still cohabitate with their estranged family members, others have moved out (or their estranged family members have moved out), or they split the use of a home where the children reside. No matter what the arrangements are, all of the homes where your client is living are likely to have a network setup with Wi-Fi in order to access the Internet. Our clients must be aware of the potential risks of sharing a home network. The risks involved could be their devices continuing to share information to other users on the network, their devices may have previously been configured to backup to a central device on the network, or other sophisticated, nefarious activities such as someone attempting to "sniff" their network traffic- in other words, attempt to see everything your client does on the Internet.

As with the living arrangements, home networks are also set up differently in all situations ranging from a very basic Wi-Fi router installed by the cable company to an extremely complex setup where an IT company is contracted to manage the devices and configuration. Although some of your clients may be tech savvy, many are not, and they need to protect their sensitive information by NOT USING the WIFI networks in the home(s) unless they have been deliberately reviewed and reconfigured by a trusted expert designated by your client. If your client does not have a newly configured home network that only their devices have access to, they should first remove access for

all of their devices which is often an option located in the Wi-Fi settings for each device such as "*forget [this] network*" or similar language. This can be accomplished whether the device is connected to that particular network or not.

Unless and until WiFi network(s) that estranged spouse / family member(s) had access to are examined and secured, clients should strongly consider the use of a dedicated Wi-Fi hotspot from their cell carrier as their exclusive means of WiFi in the home. This will allow their devices to access the Internet wirelessly over the cellular network without the risks of being attached to a shared home Wi-Fi network. In a situation where the estranged spouse / family member is still living in the home, these 'hotspots' can be further secured by 'Mac Address Restriction' which will only permit the client's device(s) to connect to them.

Apple iCloud Bleed

A common scenario in matrimonial cases where an estranged spouse seemingly has access to information from emails and / or text messages – and the client insists they were 'hacked' – turns out to be a result of what we refer to as "iCloud bleed" or spillover. This occurs when your client has their Apple iCloud logged in on various devices such as an "old" forgotten device such as an iPad or MacBook, that the estranged spouse has physical access to, or the client has entered their Apple ID credentials into a device that is utilized by one of the children – and the estranged spouse has access to that device. This inadvertent access can go on for a long period of time if your client is unaware of how to correct it which can simply be done as long as they have access to, and control of, their Apple iCloud account (i.e. Apple ID). Similar to reviewing account settings as noted above, Apple settings can be reviewed from device where the Apple ID is logged in and within the settings is a comprehensive list of "trusted devices" that use that Apple ID. By default, when these devices were logged in with your client's Apple ID, much of their information synced to these devices and continues to sync in real-time.

Sometimes there is a legitimate reason for your client's device to be used by a family member, such as a child, however Apple's Family Sharing should be setup and configured so each child has their own Apple ID and your client's Apple information is not inadvertently exposed.

Apple also recently released several new features to assist their users with protecting their sensitive information. One feature is called Advanced Data Protection for iCloud, and when enabled, allows a user's trusted devices to retain sole access to the encryption keys for the majority of their iCloud data, thereby protecting it with end-to-end encryption. In practical terms, this puts the control of even more Apple data into the user's hands as opposed to Apple controlling authentication to the data.

Another Apple feature released with the latest OS updates (iOS 16, iPadOS 16, and macOS Ventura) is Lockdown Mode. Lockdown Mode is an optional, extreme protection that's designed for those individuals who, because of who they are, what they do, or in this case – the litigation they are involved in - might be personally targeted by sophisticated digital threats. While this feature does provide an extreme level of security for Apple devices - Lockdown Mode should only be used in

extreme cases as the client's device(s) will not function like normal and many features will be extremely limited for security and some may not be available at all.

Social Media

An area not typically focused on during a family or matrimonial matter when considering cybersecurity is social media. Social media platforms such as Facebook, Instagram, Twitter, Snapchat, and TikTok are extremely prevalent and used very often by some of your clients. As stated above, security and privacy settings should be reviewed in detail and updated, if needed. Even further, your clients should review their "friends" or "connections" as they may want to remove individuals who they do not want to share information with. And lastly, your clients should think before they post. Poor judgement and improper use of social media platforms during family law litigation can lead to very negative outcomes for your client. It is very common for social media posts to be admissible during litigation and considered when making decisions in family law matters.

If you have clients that actively engage in social media, they should consider the following guidelines

- Fully secure their accounts with new passwords and MFA
- Review their "friends" list and remove those that are no longer necessary
- Never share private information regarding their case
- Never discuss the issues or rulings made during a case
- Never disparage the opposing party

Your clients should also understand that once something is posted on social media, it is in the public domain forever, even if they "delete" it.

Section 4 Resources:

Department of Defense Best Practices for Securing Your Home Network (2023): https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF

Apple Family Sharing: https://support.apple.com/en-us/HT201060

Apple Advanced Data Protection for iCloud: https://support.apple.com/guide/security/advanced-data-protection-for-icloud-sec973254c5f/web

Apple Lockdown Mode: https://support.apple.com/en-us/HT212650

Section 5 – Digital Espionage Considerations

Many of the recommendations previously laid out are largely considered information security best practices that will inherently protect your clients from having their sensitive information exposed. However, they should also be mindful that they may be dealing with an opposing party that has the means and desire to attempt to gain access to their information through extreme measures.

In order for clients to best position themselves to avoid being a victim of targeted digital espionage, all of the aforementioned best practices should be instituted as early as possible, and clients must remain vigilant during the entire pendency of the case, and beyond. (The long term benefit is that after the threat(s) related to their case are over, their enhanced cyber hygiene will become second nature and they will be at much lower risk from cyber threats in general).

In addition to Apple iCloud "bleed" and monitoring of information over Wi-Fi networks, some of the most prevalent methods used to conduct digital espionage are:

- *Clandestine Imaging* – Covert copying of all data from computing devices in a marital residence (or shared office)
- *Spyware* – Computer and smartphone information access using illegitimate "spyware" programs
- *Legitimate apps exploited for 'spying'* – Computer and smartphone information access using legitimate apps such as message forwarding or child monitoring apps
- *Account Hacking* – Using known information and/or social engineering methods to gain unauthorized access to accounts

Clandestine Imaging

This refers to the copying, forensic imaging, or 'cloning' of a client's devices (desktop, laptop, tablet, phone, etc.) by the other party or someone acting on their behalf. With physical access to these devices the threat of the device being 'imaged' is very serious, as the party who does this will wind up with all the data from the imaged device – including deleted data, and other forms of data not even readily available to the actual user of the device, such as Internet search history and deleted browser activity.

While imaging a device may be legal in some circumstances, it is something that clients should do everything possible to prevent, for obvious reasons.

The most obvious way to prevent this type of espionage is to prevent the other party from having any form of physical access to the device(s) in question. The process of imaging a computer can take 2-4 hours or more. Imaging a smartphone or tablet can usually be accomplished in about the same time, or less. Therefore, it is imperative to NEVER allow these devices to be unattended or unaccounted for, for any significant length of time.

If possible, they should be 'locked away' when not in use (and when their user is sleeping or out of the premises).

Keeping a laptop, phone, or tablet that is needed for regular use under strict 'lock and key' may not be practical. Therefore, short of keeping them constantly locked up when not actively using them, the best solution to mitigate this risk is FULL DISK ENCRYPTION (Bit locker for Windows / File Vault for Mac) along with strong passwords known ONLY to the client – and powering these devices OFF when not in active use.

Spyware

The earliest versions of "spyware" were keylogger programs, so named because their primary function was to run quietly in the background, unseen by the user, and record every keystroke typed on the computer.

Computer spyware has become far more sophisticated. Programs such as "Realtime-Spy," "SpyAgent," and "SpyAnywhere," just to name a few popular examples, not only capture keystrokes, but can record virtually all activity conducted on the target computer, including all Internet activity and emails sent and received, audio and webcam recordings if the target device has a built-in or external webcam or microphone, all files and documents accessed from the time of spyware deployment, and more. This information is then silently relayed back to the person who installed and configured the spyware, usually through a third-party website where the 'perpetrator' has set up an account for this purpose.

Keylogger programs are generally tricky to locate, and many of the newest versions of computer spyware can avoid detection by virtually all commercial anti-virus and anti-malware scanners on the market. The only reliable way to detect their presence is through comprehensive, resource intensive forensic examinations which can cost upwards of $3,500 per device.

It is therefore more cost effective, and a safer alternative, to ***stop using any computer suspected of compromise, and replace it with a brand new one.*** Critical, ***non-executable***, user created files (i.e. – no programs) from the 'suspect computer' may be backed up, scanned to ensure they are safe, and then may be copied onto the new computer.

Preventing the deployment of targeted spyware on the new computer, in a home that the adverse spouse lives in or has access to, can be accomplished by following the suggestions above for securing devices against physical access. ***If the bad actor cannot access the device – they cannot install any spyware***.

Even more prevalent now than computer spyware, are similar programs specifically designed for deployment on smartphones. They are inexpensive, readily available on the Internet, and easy to deploy. ***If the bad actor has physical access to an unlocked device / or credentials to an iCloud account (Apple devices only)***, the inflicted damage on the victimized party, legally, strategically, and emotionally, can be devastating.

Smartphone spyware such as "Cocospy," "mSPY," and "FlexiSpy" just to name a few, give the perpetrator real-time remote access to the target device, allowing them to intercept text messages, emails, and online activity such as social media messaging. ***Some of these programs can also record the victim's phone calls and allow the perpetrator to remotely turn on the***

microphone and webcam of the target phone whenever they wish. This effectively turns the target phone into a 'room bug' – which the victim is unwittingly carrying everywhere they go – including meetings with their attorneys – which the perpetrator would undoubtedly know about, since they can access the victim's call history, texts, emails, etc. Most of these programs will also allow the perpetrator to track the exact location of the target phone through its GPS chip, providing real time information on where the targeted phone is at all times.

Generally, the perpetrator needs physical access to the device to deploy these types of spyware. However, it is important to note that it is still possible to deploy spyware remotely to Apple devices, and with less features, just by knowing the iCloud account credentials associated with the targeted device. Spyware like "Cocospy" do this by monitoring iCloud backups instead. iCloud backups usually get updated every time the device is plugged in and has Wi-Fi access, so although the spying isn't exactly "real-time," it is still there for the perpetrator to utilize. Nonetheless, for most of these programs to work in their entirety and be deployed on an iPhone or Android Device (which make up the vast majority of the mobile device market), the targeted device needs to be 'jailbroken' or 'rooted'[1].

Jailbreaking or rooting a mobile device generally requires physical access to an unlocked device.[2] In common situations, this is extremely unlikely – since most people do not leave their phones unattended in public or places where 'hackers' can have unsupervised physical access to them. In a matrimonial case, however, where the parties are cohabitating, this may present a serious risk if any device or any crucial account information is left unattended, and is not locked (i.e. password/PIN protected).

It is relatively easy using forensic tools to determine if an Apple or Android device is jailbroken or rooted. If it is not, we can be reasonably certain these types of spyware programs are not present on the device. If it is, and the owner of the device is not responsible for the jailbreaking or rooting, we can be reasonably certain that someone has done so for the purpose of installing spyware. (There are reasons, other than the installation of spyware, why someone might jailbreak or root their mobile device. For example, it is common among adolescents who wish to run unauthorized or free apps on their device.)

When a smartphone is determined to have been jailbroken by someone other than its owner, a thorough forensic examination is warranted. Such an examination can detect the presence of

[1] The operating systems of modern mobile devices such as Apple and Android, are 'locked' or encrypted, and inaccessible to all but the manufacturers. In addition to protecting their proprietary operating systems, this is done, ostensibly for security reasons, to prevent any 'apps' (software) not expressly authorized (and security tested) by the manufacturer, to be installed and run on the device. This would of course include mobile device spyware programs such as those mentioned above. Jailbreaking an iPhone or 'rooting' and Android device is a process by which the 'lock' on the operating system is broken, to the extent of allowing unauthorized 'apps' to be installed and run on the device.

[2] There are a few documented examples of phones being remotely jailbroken or rooted. However, to this author's knowledge, the technology to do so is not currently available to anyone outside the government and is extremely expensive and unlikely to be used in the scenarios discussed herein at least as of now.

the spyware, identify the specific spyware program(s) in question, and preserve evidence regarding when it was installed, what it is doing or has done, and potentially, who is responsible for installing it. To be clear, this requires a very intensive, and time-consuming forensic examination that will cost thousands of dollars.

The less costly (by far) yet still effective solution is to get a new mobile device and stop using the old (potentially infected) device. This of course eliminates any potential to recover forensic evidence of the compromise.

Once the device is removed from the cellular data network it is on (e.g. Verizon, AT&T), ***and the device is placed in AIRPLANE MODE and WiFi is turned off*** to ensure that it will not connect to any available Wi-Fi or other networks – the device may be safely accessed by the owner for the sole purpose of 'looking up' historical data or information saved on the device (e.g. contacts). ***Any attempt beyond this, to extract data from the device and transfer it to any other device, should be done by a professional.***

Once a new device (or one that has been determined to be free of compromise through professional examination) is in use, that device must be protected from compromise, as discussed above. In addition, the following recommendations should be considered:

- Choose a six-digit lock code (as opposed to a 4-digit pin) – or enable fingerprint scan access on devices that support it.
- Set the 'automatic lock' feature to lock the phone after 1 minute of inactivity.
- If using an Apple device, be sure to change your iCloud password, sign out of all currently logged in devices, and remove any untrusted or "old" devices.
- Make sure the phone is on your person or locked at all times.
- Never, never, let anyone else use or have access to the phone for any reason.

It should be noted that on February 2, 2023, New York Attorney General Letitia James secured $410,000 in penalties from a NY based software company owner for illegally promoting spyware that allowed individuals to monitor another person's device without their awareness. The software products sold by sixteen (16) different companies allowed users to secretly monitor activity on another device and led customers to believe that using their products for spying was legal, however, installing and using spyware to monitor another adult's mobile device without their consent violates numerous state and federal laws.

Legitimate Monitoring Software

It is becoming incredibly common to see parties utilizing otherwise 'legitimate' apps and services to illicit ends. For example, Verizon Wireless provides a service known as "Message+" to its wireless customers, upon request. This service allows the user to 'slingshot' their text messages to multiple devices – not through an app on the phone – but through a service provided by Verizon. If a bad actor has even brief access to the client's mobile device – they can, within minutes, quickly sign up

for this service from the client's device, enter the additional location / device the client's texts should be sent to – and then quickly deleting the 'confirmation' text sent by Verizon regarding this activation. Once enabled, there is nothing on the phone itself that would alert the client this is occurring – they would only know this if they carefully checked their Verizon Wireless online account and noticed the service had been enabled.

"PhoneLeash" is another example. This is an app specifically designed to run on Android devices. Once installed, it enables the user to send duplicate messages to another phone, or to an email address. Although this app would seem to have legitimate uses – which is why it can be installed without rooting the phone – it actually disappears into the background once it is running – making it very unlikely that the user would detect its presence if they were not the person who set it up.

Both of these examples, and others like them, can be avoided by following the strict access protocols spelled out above for security of smartphones.

Additionally, there are programs and apps designed to be used for child monitoring, so parents have a deeper understanding of what their child is doing on their devices, where they are physically located, or who they are talking to. This software can also be used for nefarious purposes by an estranged family member in order to gain access to information about your client without authorization. If your client is aware of child monitoring software previously being used for legitimate purposes, they should ensure none of their devices have this software installed.

Account Hacking

While actual 'hacking' of accounts is rare – compromise of these accounts is common and usually due to an adverse spouse obtaining (or already having) the client's username and password for these accounts. Following the information security best practices in the sections above is key to preventing account hacking. In addition, the following measures should also be taken:

- Use a completely different, secure computer such as one owned by another trusted family member or friend.
- Use your cell phone's hotspot feature to create a Wi-Fi connection for your devices if you do not have a dedicated cellular hotspot device.
- Create a new webmail account that does not include any personal identifiers in the handle, such as your name, and use this for private communications going forward. Do not access the newly created email address from any device that could have been compromised.
- Disable Bluetooth on all devices when not being used. If absolutely necessary, connect Bluetooth device(s) and then disable "discovery" (choose "make device not discoverable") so the client's device(s) cannot be detected with a Bluetooth scan.
- Do not connect any new device(s) to any old devices for any reason.
- Do not insert or use any USB drives or other removable media except those purchased new or examined and certified 'clean' by a professional (simply plugging in an infected USB drive could completely re-infect an otherwise new, clean device).

- Scrutinize all incoming email carefully. Do not open emails or attachments, or click any links contained in any email messages, except from known / trustworthy sources

Advising Clients About the Implications of 'Digital Espionage'

Clients may ask about the legalities of engaging in 'self-help' to collect digital information in connection with a matrimonial or custody case – ***but whether they do or not, counsel would be doing them a service by counseling them early on regarding the potentially serious civil and / or criminal implications of their doing so in many circumstances***.

Collection and preservation of ESI without the knowledge of all parties – for example, the clandestine imaging of a computer in the marital residence, is legal in some situations (*see e.g.* Byrne v. Byrne 650 N.Y.S.2d 499 (Kings Supreme 1996)). However, many of the methods employed by parties in matrimonial and custody cases to obtain this same type of information are not. ***Any method that involves for example, the 'interception of electronic communications' violates New York and Federal criminal laws*** (*see* NY Penal Law § 250.05 "Eavesdropping" (a class E felony); the Federal Wiretap Act 18 USC § *2510 et seq.)* – and implicates the suppression provisions of NY CPLR § 4506 – which provides that any information obtained in violation of NY Penal Law Article 250 is inadmissible in any legal proceeding in the state of New York). Furthermore, the federal Wiretap Act also provides a provide right of action for these violations AND criminalizes the 'receipt and use' of material obtained in violation of the federal Wiretap Act (see 18 USC §§ 2511; 2520).

A key factor here is to distinguish between the collection and preservation of data which is already present on a computing device the client has legitimate access to – from the unlawful interception of electronic communications – even those being sent or received on the very same 'family computer' in the marital residence. The former is legal and appropriate in the limited circumstances outlined in the relevant case law (e.g. Byrne) - while the latter is a potentially serious crime under the New York and federal law, will result in evidence that is inadmissible, and also result in civil liability.

Computer "spyware" which captures and records (i.e. intercepts) the computer usage of a party is criminal in any situation where the consent of at least one party to the communication is lacking.

Monitoring of A Child's Communications – the issue of Vicarious Consent - a Potentially Serious "Parent Trap"

Concerned and conscientious parents have a well-grounded desire to know who their kid(s) are talking to online (and on the phone) and what is being said. Is their child being bullied? Are they bullying someone else? Are they talking to some sexual predator posing as another kid? What are they really doing online? In this context, it has been held that a parent does indeed have the right to 'vicariously consent' to this monitoring or interception of their minor child's communications with a third party. However, that right is NOT absolute – and it is intensely dependent on the facts and circumstances of the situation at hand.

Monitoring (and recording) a child's communications is only permissible where the parent has an objectively reasonable basis to believe that doing so is in the best interests of protecting the child – and NOT where the parent wishes to engage in this conduct for some other purpose – for example, collecting evidence to be used in a matrimonial case. That is unless, of course, the parent can establish that doing so was in the best interests of protecting the child.

The NY Court of Appeals has directly ruled on this issue. In People v. Badalamenti (2016 N.Y. Slip Op. 02556 New York Court of Appeals, 2016), after reviewing a series of lower court decisions on the issue, the Court of Appeals held as follows:

"*In light of the persuasive precedent from other jurisdictions and the reasoning set out above we hold that if a parent or guardian has a good faith, objectively reasonable basis to believe that it is necessary, in order to serve the best interests of his or her minor child [a minor being under the age of 18 as per the NY Domestic Relations Law] to create an audio or video recording of a conversation to which the child is a party, the parent or guardian may vicariously consent on behalf of the child to the recording.*"

The Court however went on to state:

"*Our holding should not be interpreted as a vehicle to attempt to avoid criminal liability for the crime of eavesdropping when a parent acts in bad faith and lacks an objectively reasonable belief that a recording is necessary in order to serve the best interests of his or her minor child. Penal Law § 250.05 and CPLR 4506 cannot be so easily circumvented.*"

ABOUT THE AUTHOR

With more than 30 years of professional experience in private investigations, computer forensics and law, Mr. Himonidis has participated in, conducted, and supervised thousands of investigations, computer forensic engagements, e-discovery projects, and cryptocurrency and blockchain forensic matters.

He has litigated cases in both state and federal courts, and he has conducted and managed the investigative and e-discovery phases of hundreds of cases. His investigative experience spans financial fraud, including civil RICO claims, insurance fraud, fraudulent claims against the U.S. government, and embezzlement; digital forensics of both cybercrime and "traditional" crime; and complex, high-profile matrimonial and custody cases.

Mr. Himonidis has written and lectured extensively on e-discovery, digital evidence, cryptocurrency and blockchain forensics, financial investigation, and legal and ethical issues related to expert witnesses. He has served as an expert witness in cryptocurrency matters in New York and Connecticut, and he has provided expert reports, affidavits and declarations for numerous state and federal courts. In addition, Mr. Himonidis has been appointed by the Supreme Court of New York State as a neutral digital forensic examiner and cryptocurrency expert. He is a member of the New York State Bar Association Task Force on Emerging Digital Finance and Currency and co-chair of the Nassau County Bar Association Cyber Law Committee.

He is a licensed attorney, a licensed private investigator, a Certified Fraud Examiner, a Certified Computer Forensic Specialist, and a Certified Cryptocurrency Forensic Investigator, and he holds the Chainalysis Reactor Certification (CRC) credential.

Mr. Himonidis earned a Bachelor of Science degree in criminal justice from St. John's University, where he graduated cum laude. He graduated from the St. John's University of Law with a Juris Doctor degree, magna cum laude, finishing in the top 2% of his class.

For further information contact:

Nicholas G. Himonidis, J.D., CFE, CCFS, CCFI, CRC

The NGH Group, Inc.

(516)621-6500

nhimonidis@theNGHgroup.com

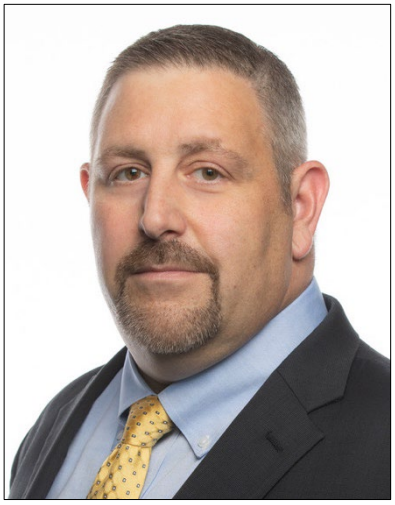
Thomas J. Foley, Esq

Tom Foley has been a partner at the law firm of Foley Griffin for 25 years. Tom primarily helps injured people in claims of negligence. As a negligence trial attorney, Tom is frequently litigating matters on behalf of the firm's clients. Tom began his legal career at the Nassau County District Attorney's office before partnering with Brian Griffin in 1997. In addition to the negligence work, Tom also provides guidance to his attorney colleagues facing complaints by the grievance committees. Tom's experience in both criminal and civil law has proven invaluable in this unique practice area. Tom also serves as an adjunct professor at his alma mater, St. John's University School of Law. Finally, Tom and his partner are hosts to the annual Massapequa Thanksgiving Day Turkey Trot, raising thousands of dollars to fight cancer.

Nicholas G. Himonidis, JD, CFE, CCFS, CCFI, CRC

President, The NGH Group

nhimonidis@theNGHgroup.com



With more than 30 years of professional experience in private investigations, computer forensics and law, Mr. Himonidis has participated in, conducted, and supervised thousands of investigations, computer forensic engagements, e-discovery projects, and cryptocurrency and blockchain forensic matters.

He has litigated cases in both state and federal courts, and he has conducted and managed the investigative and e-discovery phases of hundreds of cases. His investigative experience spans financial fraud, including civil RICO claims, insurance fraud, fraudulent claims against the U.S. government, and embezzlement; digital forensics of both cybercrime and "traditional" crime; and complex, high-profile matrimonial and custody cases.

Mr. Himonidis has written and lectured extensively on e-discovery, digital evidence, cryptocurrency and blockchain forensics, financial investigation, and legal and ethical issues related to expert witnesses. He has served as an expert witness in cryptocurrency matters in New York and Connecticut, and he has provided expert reports, affidavits and declarations for numerous state and federal courts. In addition, Mr. Himonidis has been appointed by the Supreme Court of New York State as a neutral digital forensic examiner and cryptocurrency expert. He is a member of the New York State Bar Association Task Force on Emerging Digital Finance and Currency and co-chair of the Nassau County Bar Association Cyber Law Committee.

He is a licensed attorney, a licensed private investigator, a Certified Fraud Examiner, a Certified Computer Forensic Specialist, and a Certified Cryptocurrency Forensic Investigator, and he holds the Chainalysis Reactor Certification (CRC) credential.

Mr. Himonidis earned a Bachelor of Science degree in criminal justice from St. John's University, where he graduated *cum laude*. He graduated from the St. John's University of Law with a Juris Doctor degree, *magna cum laude*, finishing in the top 2% of his class.