Asset Protection Goes Digital: Cybersecurity Safeguards for Estate Planning Advisors

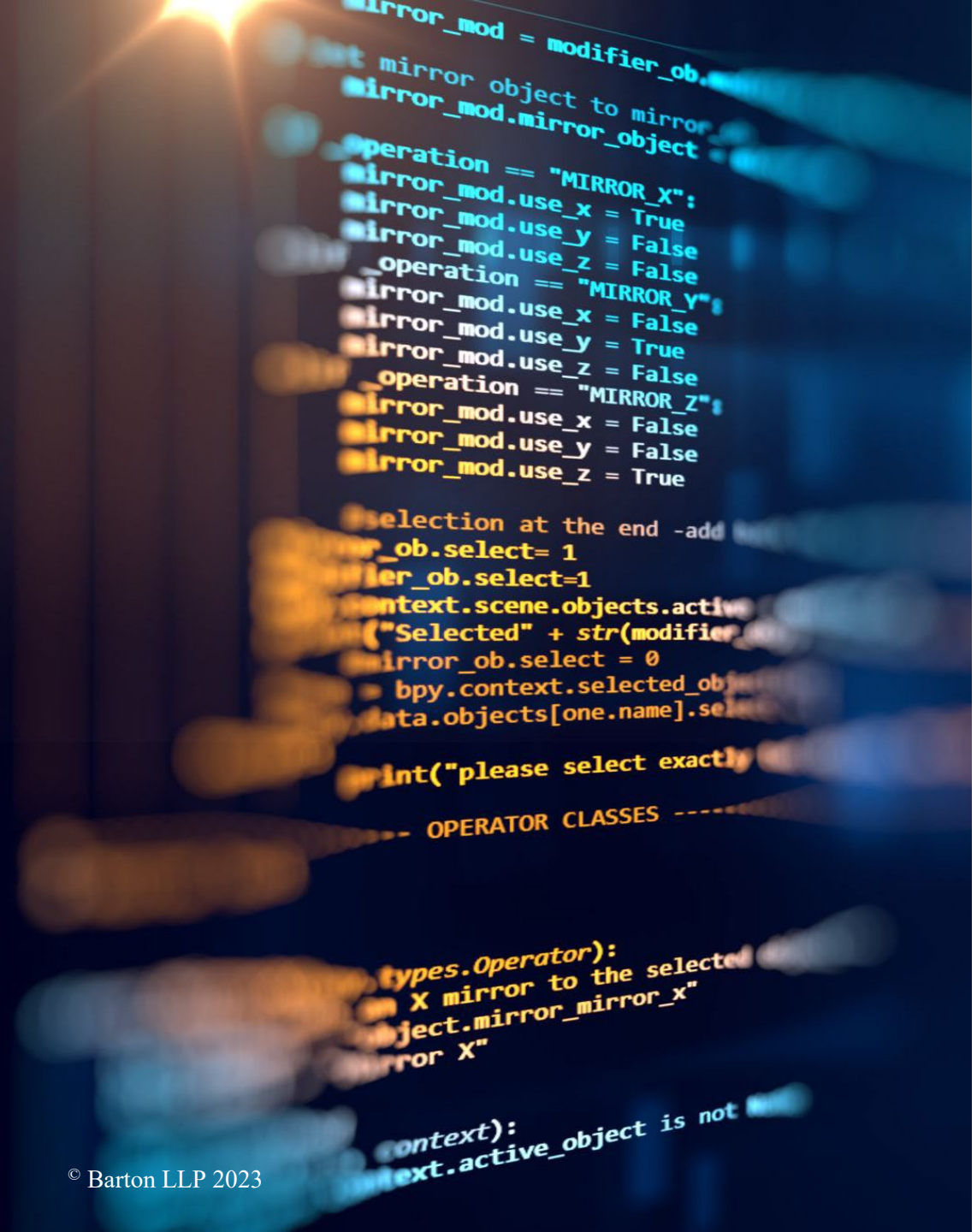
December 21, 2023

ESTATE PLANNING COUNCIL OF LONG ISLAND

Kenneth N. Rashbaum
Barton LLP
bartonesq.com

Clients Will Hire or Retain Counsel and Advisors Based on Information Security Safeguards

- Law firm network membership standards focus on law firm cybersecurity
- Association of Corporate Counsel (Data Steward Program)
- Corporations and government agencies are increasingly utilizing questionnaires and forensic audits to determine whether their law firms can keep information safe
- Can your firm pass a security audit? The answer must be "Yes"



Agenda

ESTATE PLANNING COUNCIL OF LONG ISLAND

- How and why estate planners transition form paper to safe digital asset management
- Laws and regulations stating and requiring documented cybersecurity controls
- Non-US digital asset protection
- Cyber insurance as a means to security implementation and how to save money on insurance by implementing security policies and procedures
- Attorneys: Ethics aspects of cybersecurity
- Practical suggestions for plain-English security controls the work force can understand and adopt

Estate Assets are Digital, or Linked to Digital Information

- Financial Accounts
- Cryptocurrency
- Intellectual Property
- Real Property Documents (including coop apartment shares)
- Insurance policies
  - *All are easy to obtain and send, and easy to steal*

Threat Landscape and Exposures to the Client

- Many attacks and breaches through weaknesses in third-party security
  - Multiple crypto thefts
  - Twitter (prior to rebranding as “X”)
  - AT&T
  - MGM Grand and Caesar’s Las Vegas
  - Uber
  - Multiple law firms; class actions pending against several
  - Ukraine war continues to increase the threats (crossfire between Russia and Ukraine, as in NotPetya in 2017)
  - *Many clients fear that their law firms are potential leak points, jeopardizing the client’s brand and reputation and exposing the client legally*

BARTON
Discover Better Law

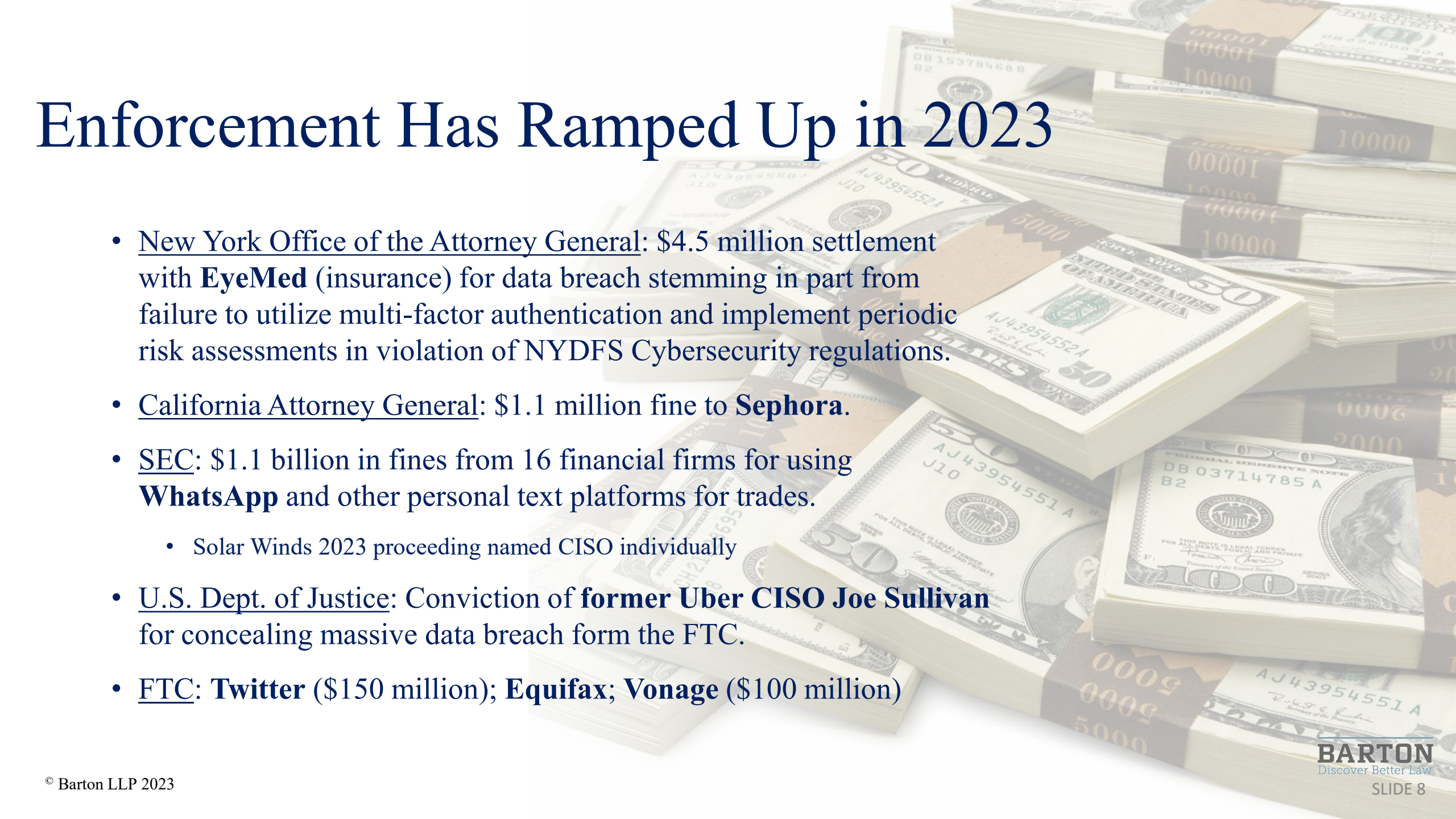
COVID Fundamentally Changed the Data Landscape

- Ransomware attacks are up 148% since the start of the pandemic
- Remote work has widened the target base for cybercriminals
- Special considerations for cyber-hygiene for remote workers:
  - Update home routers
  - Encrypt communications with protected, proprietary or sensitive information
  - Exercise caution when using public Wi-Fi
  - Set home computers to automatic security upgrades and install the most recent operating system
  - Anti-phishing awareness pop-ups
  - Silence or unplug virtual assistants

The Client's Legal Obligations in Engaging Advisors and the Client's Potential Exposure

- Cybersecurity Due Diligence in Selection of Counsel
  - New York SHIELD Act of 2019 and New York Department of Financial Services Cybersecurity Regulations (23 NYCRR Part 500)
  - Connecticut Data Privacy Act (effective 2023)
  - Colorado Privacy Act (2023)
  - HIPAA
  - California Consumer Privacy Act (CCPA) and California Privacy Rights Act (2023)
  - Virginia Consumer Data Protection Act (2023)
  - General Data Protection Regulation (EU but impacts US firms and clients who market goods or services to EU residents)
- Required data protection (privacy and security) provisions in engagement agreements: All of the above and more (US states and non-EU countries)
  - *If the firm loses protected information, the client may be primarily liable under these laws and regulations*

Enforcement Has Ramped Up in 2023



- New York Office of the Attorney General: $4.5 million settlement with **EyeMed** (insurance) for data breach stemming in part from failure to utilize multi-factor authentication and implement periodic risk assessments in violation of NYDFS Cybersecurity regulations.
- California Attorney General: $1.1 million fine to **Sephora**.
- SEC: $1.1 billion in fines from 16 financial firms for using **WhatsApp** and other personal text platforms for trades.
    - Solar Winds 2023 proceeding named CISO individually
- U.S. Dept. of Justice: Conviction of **former Uber CISO Joe Sullivan** for concealing massive data breach form the FTC.
- FTC: **Twitter** ($150 million); **Equifax**; **Vonage** ($100 million)

SEC Cybersecurity Regulations and Duty of Communication

- Two regulations
  - Proposed in February and March 2022
  - Finalized in Federal Register July 2023
- Disclosures of security incidents that would be material to an investor
- Written information security program.
- Work force training
- Regulations apply to public companies, funds, and Registered Investment Advisors

SEC Cybersecurity Risk Management Rules for Registered Investment Advisors and Funds

- Advisors and funds must adopt and implement Written cybersecurity policies and procedures including:
  - Access controls
  - Information classification
  - Malware defenses
  - Security Incident response plan
  - Threat and vulnerability monitoring and assessments

What Information Must Be Protected?

- Client requirements: Does the client ask that some or all communications with it be encrypted?
- Trade secrets, financial, proprietary and sensitive information
  - 23 NYCRR Part 500 Amendments: business information that, if accessed, would pose a "material adverse impact" to the business
- Federal and State Law Requirements:
  - Social Security and Financial Account Numbers; financial statements, including those in co-op purchase applications and matrimonial disclosures); biometric information; geolocation information)

Protected Information

- Varies between states and countries
- GDPR and CCPA: Information that can be traced to an identifiable natural person.
- Most states limit information that requires safeguards and notification in the event of a breach to:
  - Social Security Numbers
  - Drivers License and passport numbers
  - Credit card information (usually with security code or password except in MA)
  - Biometric information

Data Protection is an Ethical Requirement

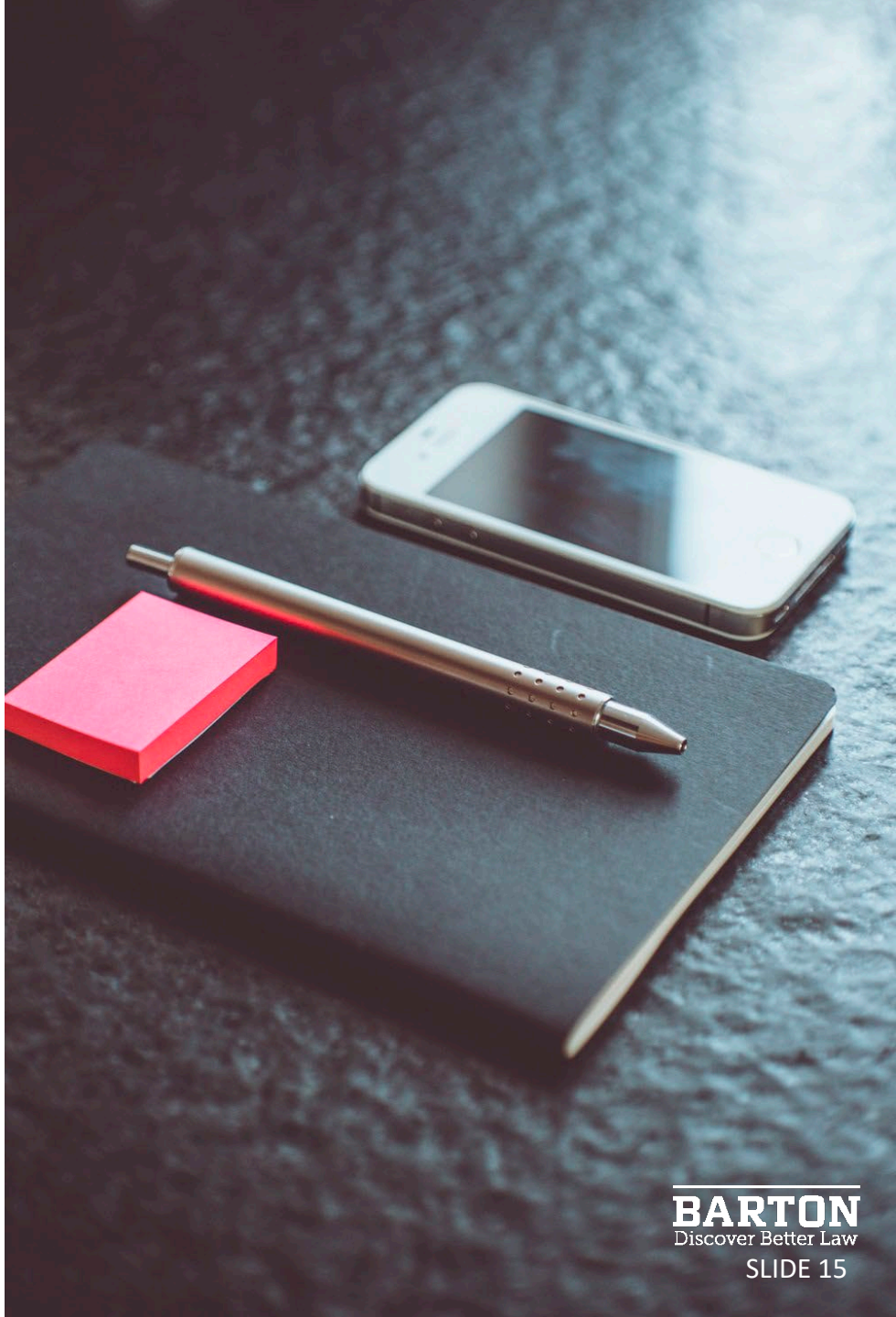
- Competence: Duty to know the technology relevant to the matter:
- ABA Model Rule 1, Competence, Comment 8: The attorney must have or acquire the technical knowledge necessary to represent the client (2012)

Legal Requirements Mandating Client Due Diligence Into Law Firm's or Other Advisors' Data Protection Posture

- GDPR
- HIPAA
- California Consumer Privacy Act
- NYDFS Cybersecurity Regulations (23 NYCRR Part 500)
- Clients may be accountable for a breach by our firm if they can't document their due diligence into our security posture
- Cyber insurers' underwriting

Beyond Competence: Communication

- Explaining the rationale for technology compliance initiatives to the Board, C-Suite and senior management implicate Rule 1.4(B)
  - "The attorney shall explain a matter to the client to the extent reasonably necessary to permit the client to make informed decisions about the representation."



No “Failures to Communicate”* Due to Lack of Technology Knowledge

- You must understand the technology in order to explain it to the senior management and the board in a way that enables them to make informed decisions
  - Data protection compliance initiatives
  - Cyber and privacy liability insurance
  - Breach response
  - Outside counsel engagement or disengagement
  - *“Cool Hand Luke” (1967)

Potential Loss of Privilege in e-Communications and Storage

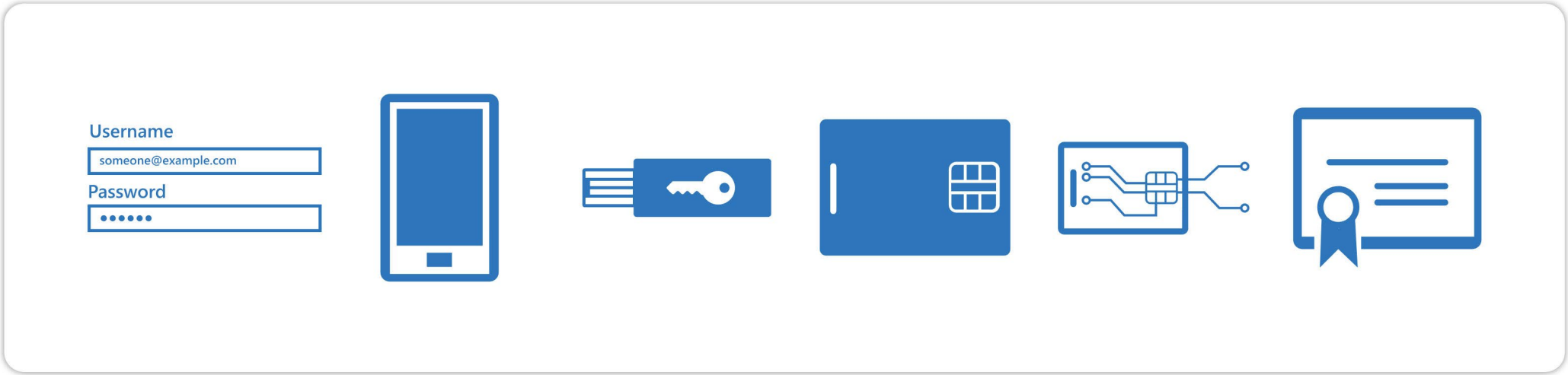
- Misdirected email or text ("autofill")
- Email sent to or from monitored and/or accessed network
  - *Scott v. Beth Israel Medical Center:* privilege lost by employee who sent email to counsel over organization network
- Lax cybersecurity safeguards can lead to cyber attacks and disclosure of privileged data (i.e., lack of "reasonable safeguards" may doom an application for returnn of privileged material under FRE 502 "Clawback")

Practical Suggestions for Data Safeguards

- Multi-Factor Authentication
  - Something you know (password), something you have (phone)
  - In 2023, a deal-breaker for cyber insurance and cyber insurance, in turn, is increasingly a client counsel requirement

Insurance Considerations

- A cyberattack is a matter of "when," not "if."
- Applications for insurance mandate documentation for security controls and underwriters will assess those controls, sometimes by remote means.
- Well-documented controls on which the work force has been trained can result in:
  - Higher limits with fewer sublimits
  - Fewer exclusions and narrow "loss" and "claim" definitions
  - More reasonable premiums



Why MFA?

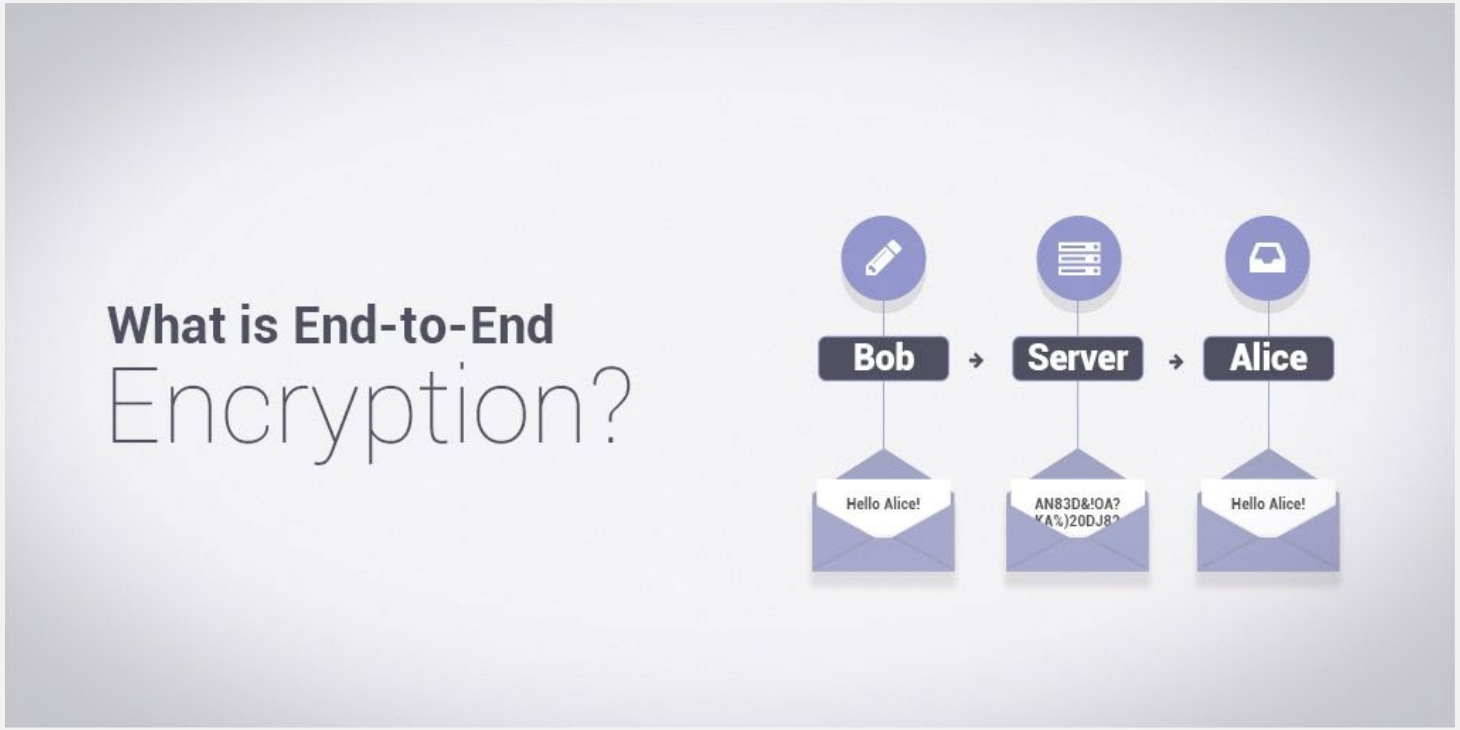
- More secure than passwords alone
- Adds an added layer of verification that only the intended for the user *so longer as the user pays attention to the alerts*
  - NYDFS *Residential Mortgage* penalty proceeding*:* employee pressed "Approve" multiple times after she was no longer at work
- Compliance with certain regulations (NYDFS Cybersecurity Regulations)

Encryption

- One of the easiest safeguards and one of the most effective
- If in doubt, encrypt the email. That will encrypt the attachment, too
- Note: All 50 states have data breach notification statutes, and 49 exempt from the notification requirement for data that is encrypted

Encryption Process

- Critical for emails containing sensitive data such as bank account numbers, SSNs, passport information, credit card information and client-sensitive information should be sent in encrypted format

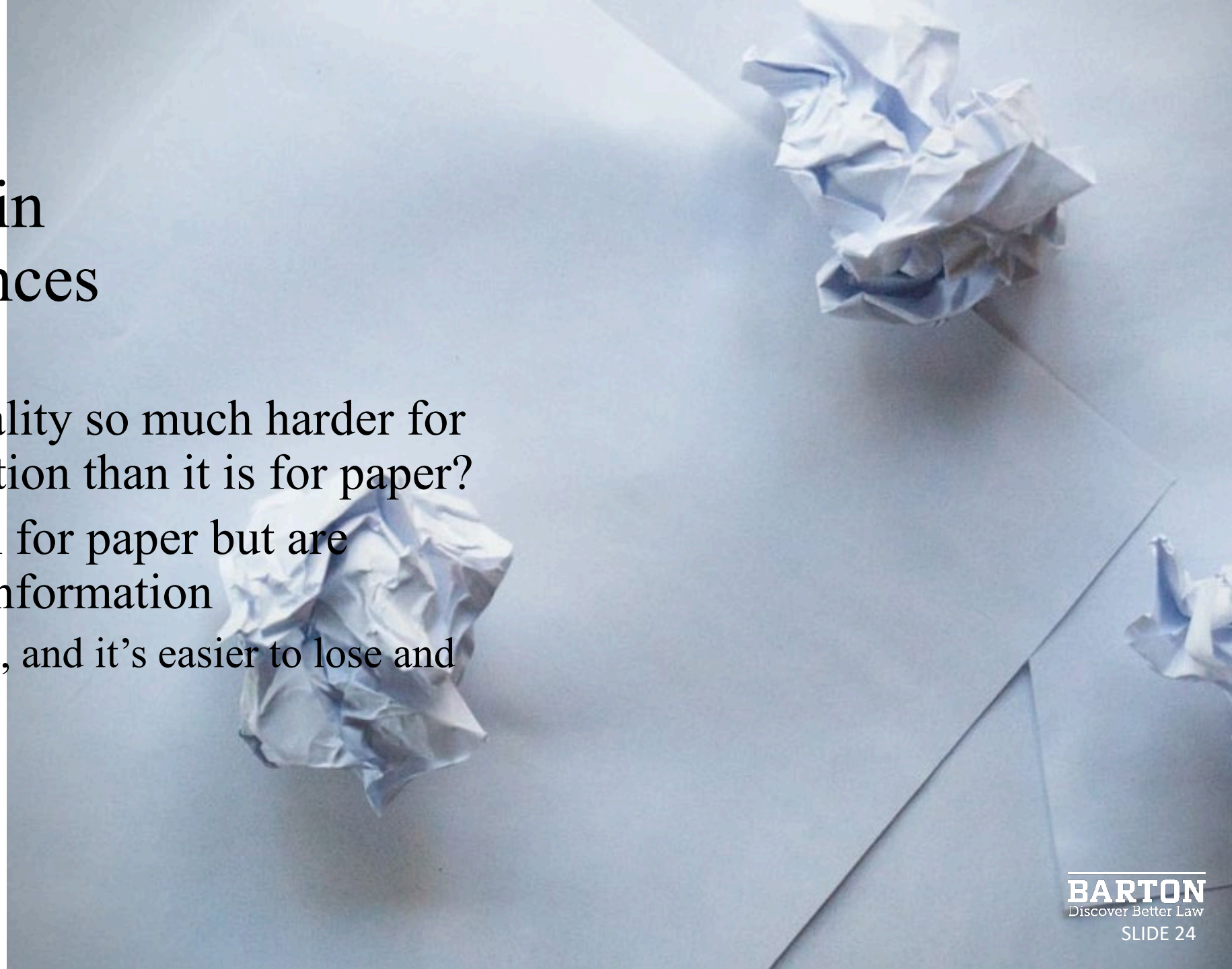


Public Wi-Fi

- National Security Administration (NSA) Guidance July 2021: Malware of increasing sophistication has been found in public Wi-Fi (airports, etc.)
- Hotel Wi-Fi may have credential-stealing malware (obtains your password and username) or may be a fake site that is in fact the hacker's site
- Suggestions:
  - Use your phone's personal hot spot (most have them for no additional cost)
  - Verizon or other mobile hot spot (Verizon "Jet Pack")
  - If it's urgent, log on and avoid sending sensitive information. Then, reboot the device

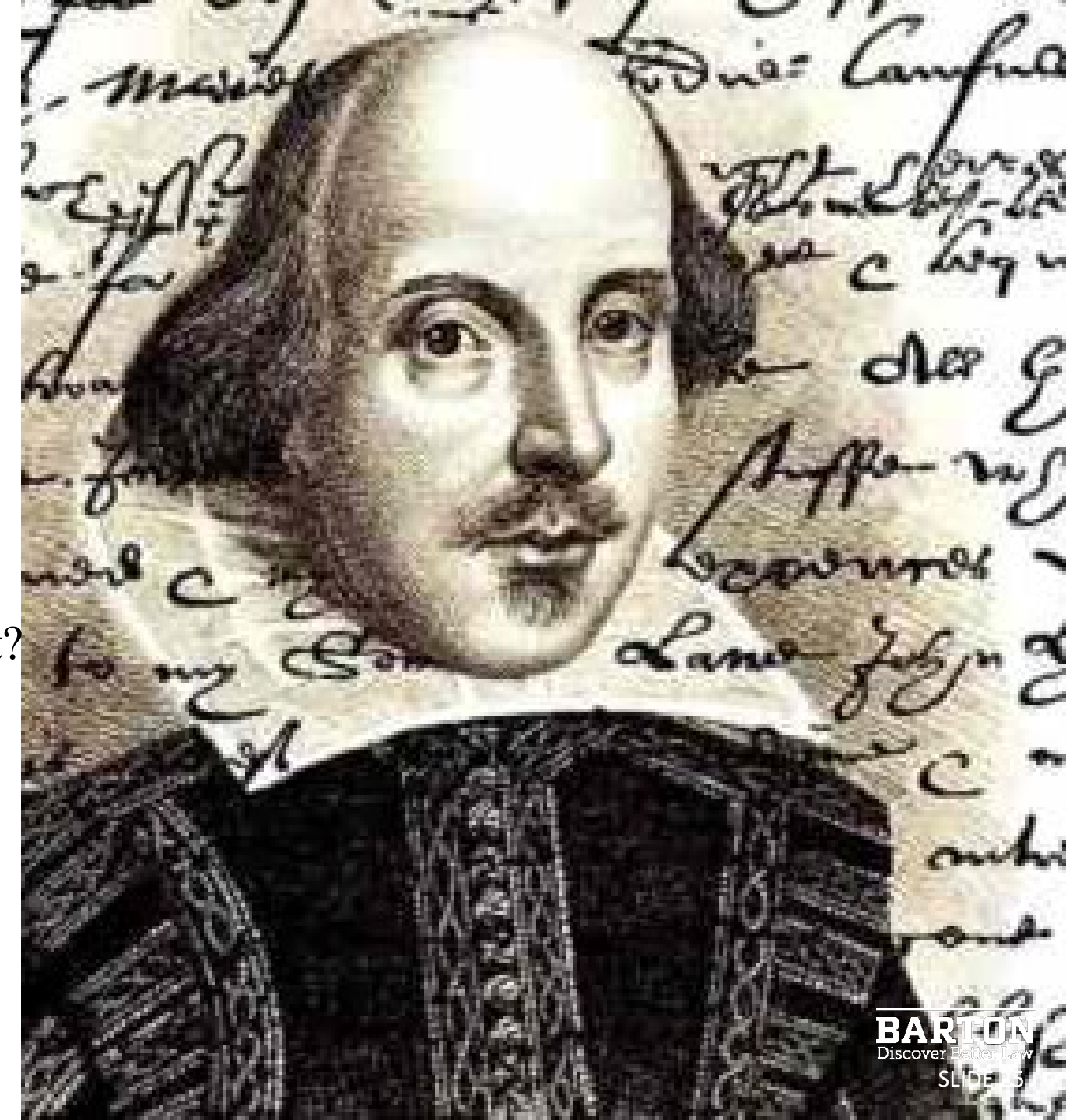
Duty to Maintain Client Confidences

- Why is confidentiality so much harder for electronic information than it is for paper?
- Rules were written for paper but are applied to digital information
  - There is more of it, and it's easier to lose and alter

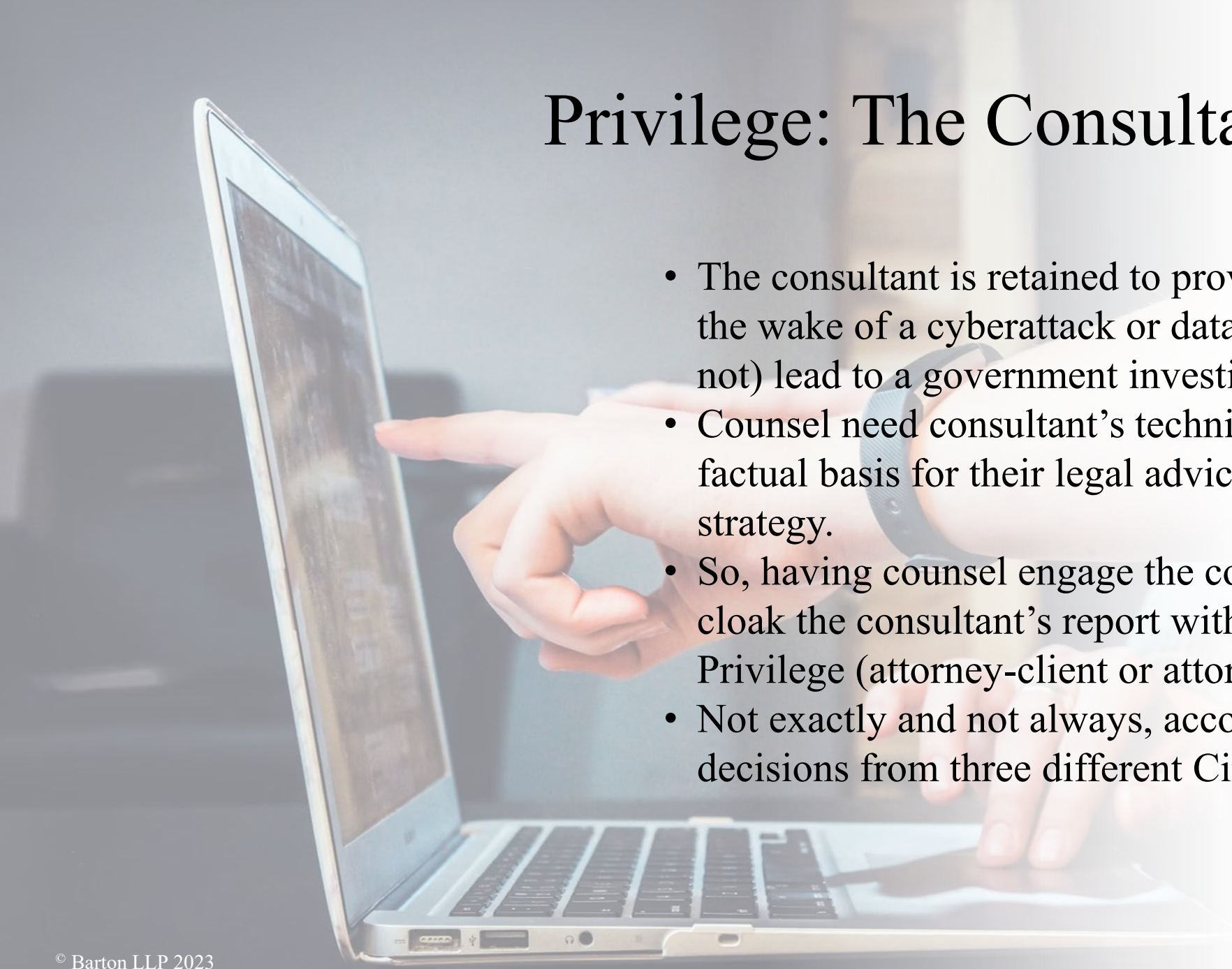


Duty to Maintain Client Confidences

- Confidentiality and written communications have had an uneasy relationship for a long time:
- “Is it not a lamentable thing that the skin of an innocent sheep be made parchment? That parchment, being scribbled o’er, should undo a man?” *Henry VI, Part 2, Act 4, Scene 2 (1591)*



Privilege: The Consultant Conundrum



- The consultant is retained to provide technical expertise in the wake of a cyberattack or data breach that may (or may not) lead to a government investigation or litigation.
- Counsel need consultant's technical expertise to provide a factual basis for their legal advice and formulation of strategy.
- So, having counsel engage the consultant is sufficient to cloak the consultant's report with Legal Professional Privilege (attorney-client or attorney work product)?
- Not exactly and not always, according to three federal decisions from three different Circuits (3rd, 4th and D.C.)

Typical Court Responses to Discovery Disputes, Including Privilege

- Judicial trend is against privilege.
- "Work it out among yourselves, counsel."
- "Just give it to her."
  - "I'll decide admissibility into evidence later."
  - How many cases in 2023 reach the admissibility question? Most settle well before that and disclosure of the report can impact settlement negotiations dramatically.

Decisions Evidence Narrowing of Privilege Concerning Cybersecurity Consultants

- *In re Capital One Consumer Data Security Breach Litigation*; 2020 U.S. Dist. LEXIS 91736 (E.D. Va. May 26, 2020), aff'd, 2020 U.S. Dist. LEXIS 112177 (E.D. Va. June 25, 2020).
- Massive breach of consumer data. Capital One asked cybersecurity consultant that had been engaged by the company previously and was on retainer to the company to investigate and prepare a report.
- Long-standing business relationship between consultant and company led court to deny assertions of privilege on ground that report was primarily business advice: company would have engaged this consultant to prepare this report regardless of potential litigation and regulatory implications.

Focus: Purpose of the Report

- Why was the report prepared? Crucial inquiry
- *Wengui v. Clark Hill PLC,* 338 F.R.D. 7 (D.D.C. 2021)
- Law firm data breach. Two reports were prepared, one purportedly for preparation for litigation (work product doctrine) and the other to address the firm's cybersecurity issues. Second report, at issue, contained details regarding technical facts of the cyberattack and consultants were referenced as "incident response team."
- "Malicious cyberattacks have unfortunately become a routine part of our modern digital world." Court held that there was no showing report wouldn't have been prepared regardless of threatened litigation.

Legal and Business Must Be on the Same Page

- *In re Rutter's Data Security Breach Litigation*, No. 1:20-CV-382, 2021 U.S. Dist. LEXIS 136220 (E.D. Pa. July 22, 2021).
- Data breach from point-of-sale payment card platform. Outside counsel engaged to advise on data breach notification obligations. Counsel hired consultant to assess the scope of the incident (i.e., number of affected individuals and their states and countries of residence).
- At 30(b)(6) deposition corporate signatory of consultant's engagement agreement testified he was unaware of potential litigation AND would have ordered the investigation even if no litigation were contemplated. Outside counsel who engaged consultant was never sent a copy of the report.
- Privilege assertion denied.

Privilege Enhancement Checklist

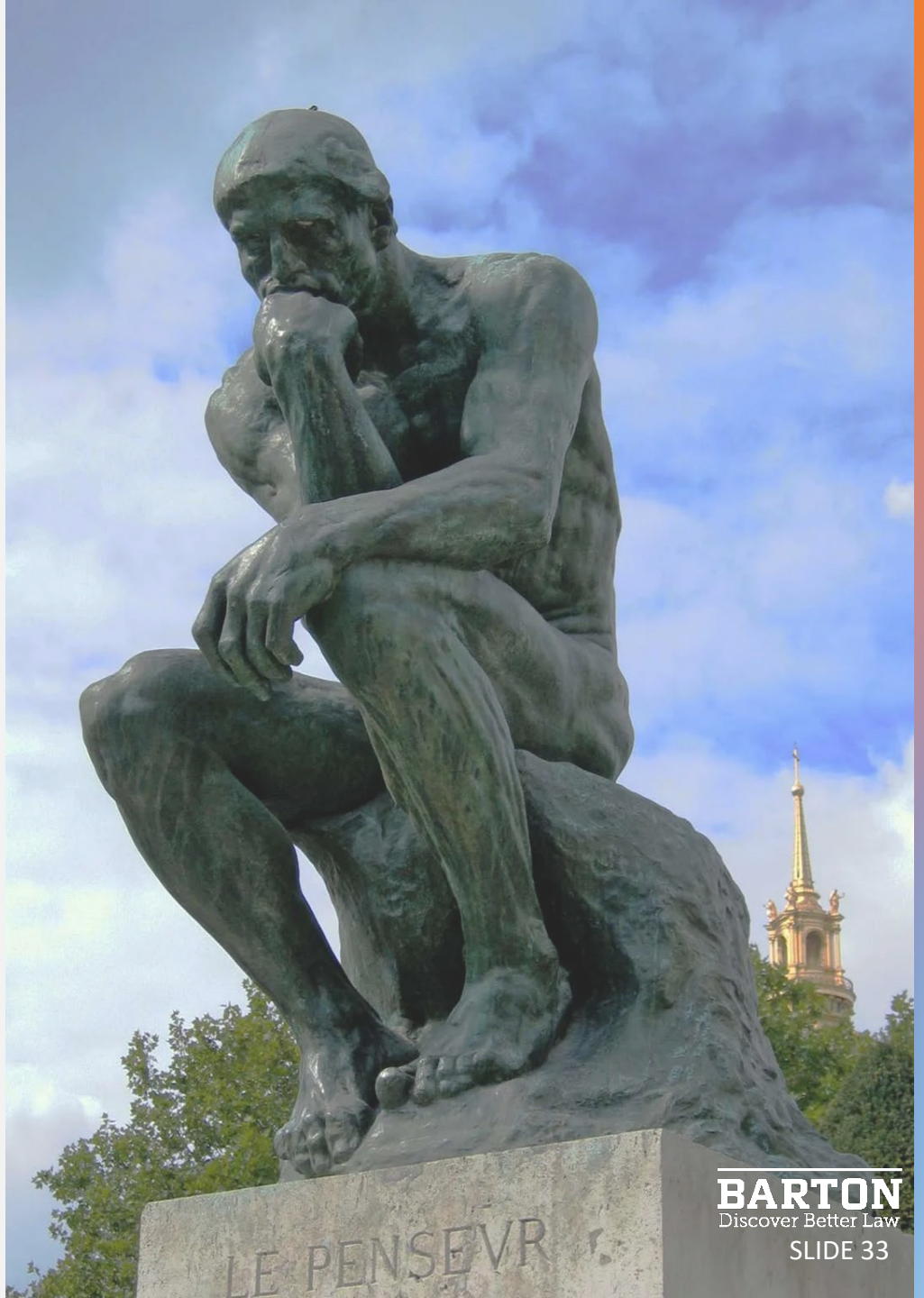
- **Caveat**: Privilege is highly fact-dependent. Document the facts assiduously.
- Try to use a different consultant/vendor than the one engaged for risk assessments, etc.
- Involve Legal early, preferably outside counsel to increase the chances of a successful privilege assertion.
- Clarify the legal advice purpose of the consultant's engagement in the engagement agreement.
  - Report should indicate the legal issue/question and state that the report will be used in formulating legal advice and strategy.

Privilege Checklist, continued

- Limit the distribution of the report ("Circle of Trust"). DO NOT forward to those outside the Circle, and **DO NOT** send as "Reply to All."
  - Exercise caution when considering whether to send the report you wish to protect to your insurance carrier. *This may be considered a waiver of privilege!*
- All communications regarding the investigation should flow through counsel (preferably outside counsel).
- Be judicious with the term "breach." It's defined in various ways across federal and state laws and may implicate business advice (breach notification obligations).
- Prepare witnesses for 30(b)(6) deposition with privilege considerations in mind.

Final Thoughts

- In Ethics and technology, “The old world is rapidly changing” (Bob Dylan)
- Considerations include the type of technology, its usage in business and law and jurisdictions involved
- Keep the business owners and senior management in the loop concerning the impact of cybersecurity controls and privacy controls on the flows of personal and company proprietary information



Kenneth N. Rashbaum

Partner

Barton LLP

(212) 885-8836

krashbaum@bartonesq.com

bartonesq.com