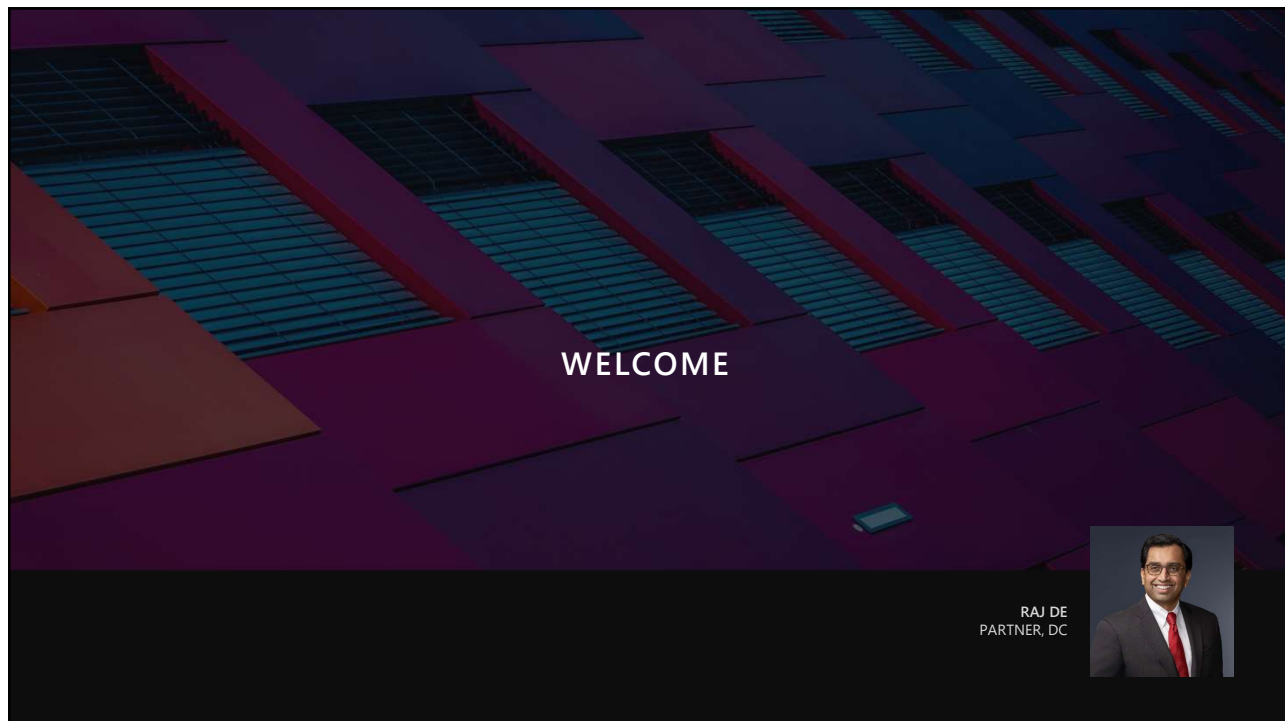




1



2

AGENDA

1. Introductions
2. AI- Powered Crime
3. Artificial Intelligence & Emerging Cybersecurity Risk
4. Reporting Responsibilities
5. Ethical Obligations for Attorneys

MAYER BROWN

3

01
INTRODUCTIONS

4

PRESENTERS



PARTNER
GINA M. PARLOVECCHIO
 NEW YORK +1 212 506 2522
 MAYER BROWN



PARTNER
JUSTIN HERRING
 NEW YORK +1 212 506 2878
 MAYER BROWN



SENIOR MANAGER DIRECTOR
JORDAN RAE KELLY
 WASHINGTON DC +1 202 312 9140
 FTI CONSULTING



DEPUTY CHIEF, NATIONAL
 SECURITY AND CYBERCRIME
ALEXANDER MINDLIN
 NEW YORK
 EDNY

MAYER BROWN

5

2024 DEEPFAKE FRAUD STATISTICS

- According to a McAfee global survey, **70 percent of people said they aren't confident that they can tell the difference between a real and cloned voice.**
- In the same survey, **40 percent of people in the same study reported they would help if they got a voicemail from their spouse who needed assistance.**
- The 2023 FBI Internet Crime Report indicated that business email compromises, one of the most common types of fraud, can cause substantial monetary loss.
 - For years, fraudsters have been compromising individual and business email accounts through social engineering to conduct unauthorized money transfers. However, with generative AI bad actors can perpetrate fraud at scale.
- The Deloitte Center for Financial Services estimates that generative AI email fraud losses could total about **\$11.5 billion by 2027** in an "aggressive" adoption scenario."
- Experts predict that generative AI is expected to significantly raise the threat of fraud, which could **cost banks and their customers as much as \$40 billion by 2027.**

PERSONAL FINANCE - BANKS

**AI is used in half of bank
scams. Here's what you
need to watch out for**

**AI Deepfakes On The Rise
Causing Billions In Fraud
Losses**

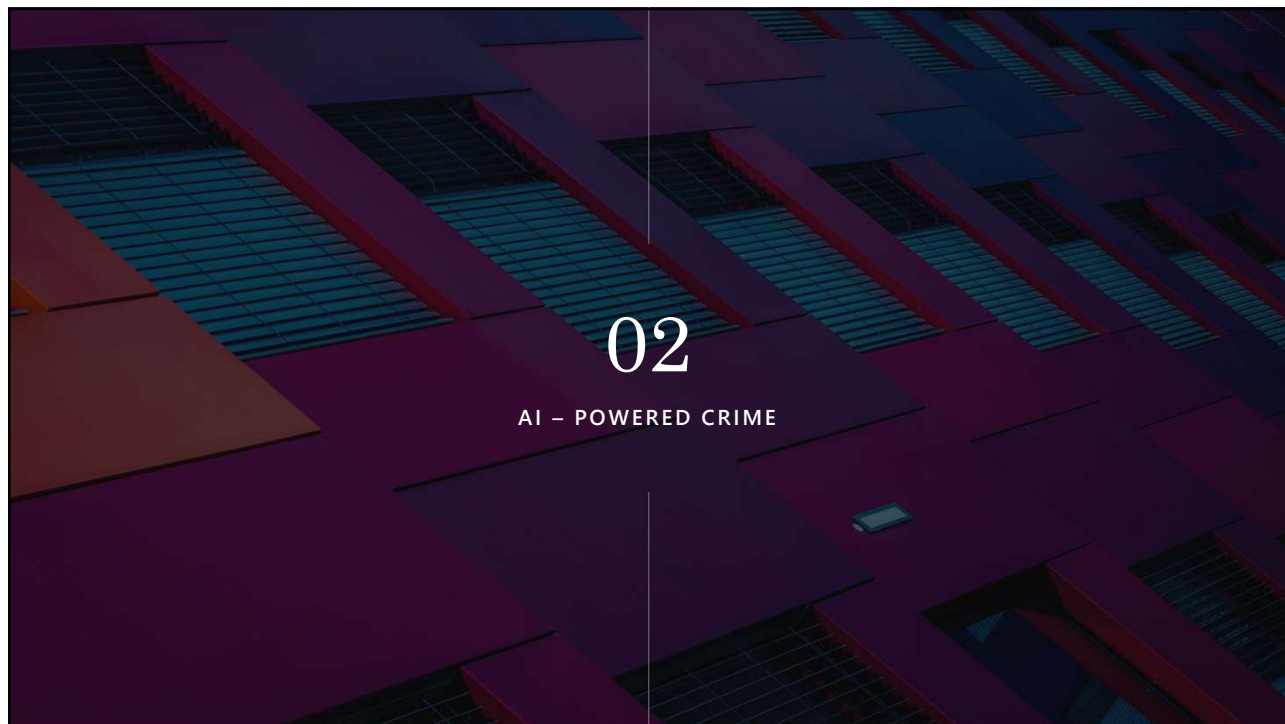
**CEO of world's biggest ad firm targeted
by deepfake scam**

Exclusive: fraudsters impersonated WPP's CEO using a fake
WhatsApp account, a voice clone and YouTube footage
used in a virtual meet

**Artificial Imposters—Cybercriminals Turn to AI Voice
Cloning for a New Breed of Scam**

MAYER BROWN

6



7

GOVERNMENT WARNINGS ON AI-ENABLED CRIME

- **Former Deputy Attorney General Lisa Monaco – Misuse of AI to Commit Crime**

- Speech on February 20, 2024 recognizing that AI is “a double-edged sword” that can accelerate risks to national security, amplify biases and discriminatory practices, expedite creation of harmful content, accelerate disinformation, and create new opportunities for cyber-related criminal conduct.
- Reference to New Hampshire election in which robocalls made in January 2024 with AI-generated voices, impersonating President Biden, discouraged people from voting in the state’s primary election.
- Acknowledged that criminal justice system “has long applied increased penalties” for certain crimes, such as those involving firearms, and “[l]ike a firearm, AI can also enhance the danger of a crime.” Thus, going forward, DOJ will seek tougher sentences for offenses “made significantly more dangerous by the misuse of AI.” If existing sentencing guidelines do not allow for such enhancements, DOJ will seek to modify those guidelines to “close the gap.” This approach, she noted, “will deepen accountability and exert deterrence.”

- **Proposed Legislation to increase penalties for the commission of financial crimes using artificial intelligence.**

- **FinCEN warns financial institutions about use of deepfake media by criminals targeting financial institutions and their customers**

- November 18, 2024, FinCEN warns of fraudsters are increasingly leveraging AI-generated deepfakes to bypass customer identification and verification and customer due diligence controls at financial institutions, and perpetrate fraud schemes and other financial crimes.

MAYER BROWN

8

AI-FUELED SOCIAL ENGINEERING



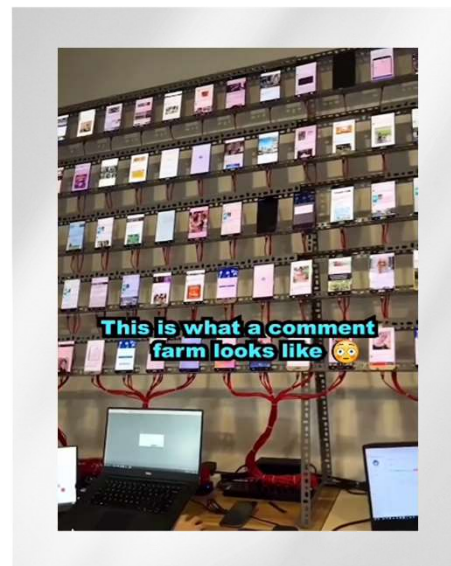
- Advances in ML and deep learning have enabled AI to create convincing fake content, like deepfake videos and video clones
 - GenAI quickly analyzes public data
 - LLM chatbots craft accurate phishing communications
 - GenAI can swiftly generate convincing phishing pages
- Phishing threats have reached unprecedented levels of sophistication in the past year, driven by the proliferation of genAI tools
- Examples of AI-powered traditional social engineering tactics:
 - Phishing and spear phishing
 - Deepfake and voice cloning
 - Automated chatbots

MAYER BROWN

9

FRAUD AT A SCALE

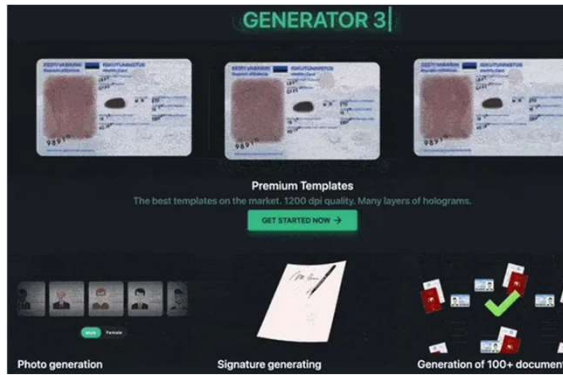
- Financial Institutions are being impersonated and customers are being defrauded
 - Logo
 - Bio text
 - Fake websites
- Means of communication include text messaging, social media contact, phone calls, phishing emails
- Advanced phone farmers use a variety of tactics to hide their activity, including hiding behind fresh IP addresses, using a broad variety of devices, and resetting their Device IDs with each install



MAYER BROWN

10

TOOLS FOR FRAUD: NEURAL NETWORK & FAKE DOCUMENTS



- Fraudsters have access to increasingly sophisticated tools through crime-vendors
- An underground website called OnlyFake uses "neural networks" to generate realistic looking photos of fake IDs for just \$15.
- Hand-crafted fake IDs are being produced in minutes with quality good enough to bypass many ID Verification tools
- Fake IDs generated by OnlyFake have successfully passed identity verification by companies

MAYER BROWN

11

FAKE AI-GENERATED EMPLOYEES

- The DPRK has dispatched thousands of skilled IT workers around the world, who use stolen or borrowed U.S. persons identifies to **pose as remote workers and infiltrate domestic companies' networks.**
- The Justice Department unsealed charges and made arrests and seizures, to disrupt the fake employee scams. In addition to data extortion, the FBI has observed North Korean IT workers:
 - Leveraging unlawful access to company networks to exfiltrate proprietary and sensitive information;
 - Facilitating cyber-criminal activities;
 - Collecting salary on behalf of the regime; and
 - Using artificial intelligence and face-swapping technology during video job interviews to obfuscate their true identities.
- In addition to data theft and extortion, fake employees can pose **sanctions issues.**



Side-by-side comparison of stock photo and the applicant's faked photo

MAYER BROWN

12

AI-POWERED CRIME

High-Concern Crimes

Audio/visual impersonation

Tailored phishing

Disrupting AI controlled systems

Disinformation campaigns

Revenue-extraction schemes

(CNN) — A finance worker at a multinational firm was tricked into paying out \$25 million to fraudsters using deepfake technology to pose as the company’s chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

There is still a lot we don’t know about the robocall in New Hampshire that [impersonated President Joe Biden](#), likely using AI voice cloning technology.

The call went out on Jan. 21, two days before the primary, trying to discourage Democrats from heading to the polls. It’s not certain who was behind the call, what software was used in its creation, or how many voters got one. The New Hampshire attorney general’s office [is investigating](#).

Hidden inside the foundation of popular artificial intelligence image-generators are thousands of images of child sexual abuse, according to a [new report](#) that urges companies to take action to address a harmful flaw in the technology they built.

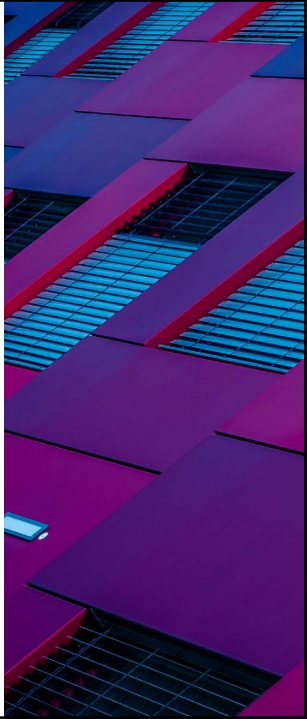
Those same images have made it easier for AI systems to produce realistic and explicit imagery of fake children as well as transform social media photos of fully clothed real teens into nudes, much to the alarm of [schools and law enforcement](#) around the world.

MAYER BROWN

13

FOREIGN ACTORS USING AI TOOLS TO ENHANCE CYBERATTACKS

- According to a Google report released on January 28th, in the past year alone dozens of hacking groups in more than 20 countries used Google’s Gemini chatbot to assist with malicious code writing, hunts for publicly known cyber vulnerabilities, and research into organizations to target
- Groups with known ties to China, Iran, Russia and North Korea all used Gemini to support hacking activity
 - The platform was used to boost productivity rather than to develop new hacking techniques
 - More than 20 China-linked groups and at least 10 Iran-linked groups were seen using Gemini
- Iranian groups used Gemini for research into defense organizations to target with hacking attempts and generation of content in English, Hebrew, and Farsi to be used in phishing campaigns
- China conducted reconnaissance on targets in addition to attempting to learn more about specific hacking tactics, including how to exfiltrate data, evade detection and escalate privileges once inside a network
- North Korea used Gemini to draft cover letters for research jobs and Russia used the tool to for mostly mundane coding-related tasks



14



15

NYDFS
INDUSTRY
LETTER ON
CYBERSECURITY
RISK ARISING
FROM AI

- On October 16, 2024, the New York State Department of Financial Services (DFS) issued an industry letter, *Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks*.
- The DFS guidance identifies four primary cybersecurity risks arising from AI: two caused by threat actors' use of AI, and two caused by a Covered Entity's use of AI.
 - **AI-Enabled Social Engineering:** Covered Entities are confronting a surge in social-engineering attacks that use new AI tools to create realistic and interactive audio, video, and text.
 - **AI-Enhanced Cybersecurity Attacks:** Threat actors can leverage AI tools to scan for and exploit vulnerabilities, conduct reconnaissance, accelerate malware and ransomware deployment, and evade detection.
 - **Exposure or Theft of Vast Amounts of Nonpublic Information:** Covered Entities may benefit in several ways from deploying AI. But this creates new risks, as many AI tools require the collection and processing of large amounts of sensitive business and personal information.
 - **Increased Vulnerabilities Due to Third-Party, Vendor, and Other Supply Chain Dependencies:** Covered Entities must often rely heavily on third-party vendors to deploy AI.
- The guidance outlined mitigations, including **Risk Assessments and Risk-Based Programs, Policies, Procedures, and Plans, Third-Party Service Provider and Vendor Management, Access Controls, Cybersecurity Training, Monitoring and Data Minimization**

MAYER BROWN

16

DOJ GUIDANCE ON EVALUATING CORPORATE COMPLIANCE PROGRAMS IN THE AGE OF ARTIFICIAL INTELLIGENCE

- In September 2024, the DOJ released guidance on factors prosecutors should consider in evaluating corporate compliance programs in the specific context of criminal investigations. When discussing artificial intelligence, guidance suggests prosecutors assess how companies:
 - **Manage of emerging risks to ensure compliance with applicable law**
 - Does the company have a process for identifying and managing emerging internal and external risks that could potentially impact the company's ability to comply with the law, including risks related to new technologies;
 - How does the company assess the potential impact of new technologies, such as artificial intelligence, on its ability to comply with criminal laws;
 - Is the management of risks related to the use of AI and other new technologies integrated into broader enterprise risk management (ERM) strategies; and
 - What is the company's approach to governance regarding the use of new technologies such as AI in its commercial business and in its compliance program.
 - **Engage in meaningful efforts to review its compliance program**
 - If the company is using new technologies such as AI in its commercial operations or compliance program, is the company monitoring and testing the technologies so that it can evaluate whether they are functioning as intended and consistent with the company's code of conduct; and
 - How quickly can the company detect and correct decisions made by AI or other new technologies that are inconsistent with the company's values.

MAYER BROWN

17

ARTIFICIAL INTELLIGENCE & CYBERSECURITY



MAYER BROWN

18

AI & CYBERSECURITY

- Use of large language models and deepfakes to improve **social engineering**
- Employing deepfakes to trick workers or gather intel on security team in the midst of **incident response** effort
- **Accelerate attacks** by making it faster to execute simultaneous attacks and speed up post-exploitation activities, such as lateral movement and reconnaissance
- Accelerate and reduce cost for the **development of malware** and other hacking tools

Microsoft and OpenAI say hackers are using ChatGPT to improve cyberattacks



A number of nation-backed groups are starting to use large language models to help with research, scripting, and phishing emails.

By Tom Warren, a senior editor covering Microsoft, PC gaming, console, and tech for The Verge. Warren is also dedicated to Microsoft news before going 'The Verge' in 2012.

FEB 19, 2024, 7:50 AM EST

Comments (3 New)

Photo by Amelia Hildreth-Knox / The Verge

If you buy something from a Verge link, Vox Media may earn a commission. [See our ethics statement.](#)

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

MAYER BROWN

19



20

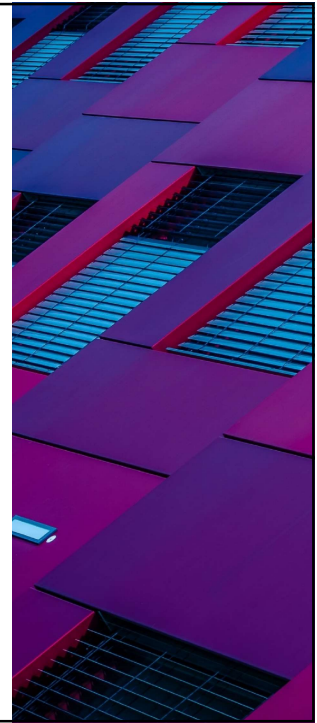
REPORTING RESPONSIBILITIES AFTER A CYBER INCIDENT

50-State Data Breach Notification Laws

Other Regulatory Notice Rules

- SEC Public Disclosure Rule & Reg S-P Notice Requirement
- New York Department of Financial Services (NYDFS)
- FFIEC Notice Rule for Banks
- State Insurance Regulators
- State Banking Regulators
- Pending Cyber Incident Reporting for Critical Infrastructure Act (CIRCA)

Preparation is Key



21



22

ETHICAL OBLIGATIONS – DUTY TO PROTECT ELECTRONIC DATA

- In 2017, ABA issued [Formal Opinion 477: Securing Communication of Protected Client Information](#)
- Lawyers must “**exercise reasonable efforts when using technology in communicating about client matters,**” and applies a reasonable efforts standard as adopting a “**fact-specific approach to business security obligations.**”
- Some factors assessed to determine if reasonable efforts were made may include:
 - The sensitivity of the information;
 - Likelihood of disclosure if additional safeguards are not employed;
 - The cost of employing additional safeguards;
 - Difficulty of implementing the safeguards; and
 - The extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use.)
- As technology has advanced, bar associations and legislators have worked to clarify lawyer’s obligations with respect to electronic data.

NEW YORK STATE BAR ASSOCIATION COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer’s obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client’s information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Topic: Confidentiality; Remote Access to Firm’s Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Topic: Duty to protect client information stored on a lawyer’s smartphone

Digest: If “contacts” on a lawyer’s smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with a smartphone app unless the lawyer concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client’s consent.

MAYER BROWN

23

ETHICAL OBLIGATIONS – CYBERSECURITY INCIDENTS

- In 2018, the ABA issued [Formal Opinion on Lawyer’s Obligations after an Electronic Data Breach or Cyberattack](#)
- In compliance with the Model Rules of Professional Conduct, this opinion covered data breaches that involve information relating to the reputation of the client. The ABA indicated that:
 - Law firms should employ **reasonable efforts** to monitor the security of their information;
 - Lawyers should “**act reasonably and promptly to stop the breach and mitigate damage from the breach**”;
 - Law firms should have **data breach plans in place** in order to remediate cyber intrusions; and
 - **Not all cybersecurity incidents require client notification.**
 - In cases where an intrusion does not gain access, client confidential information doesn’t need to be disclosed.
 - However, disclosure is required if “**material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.**”

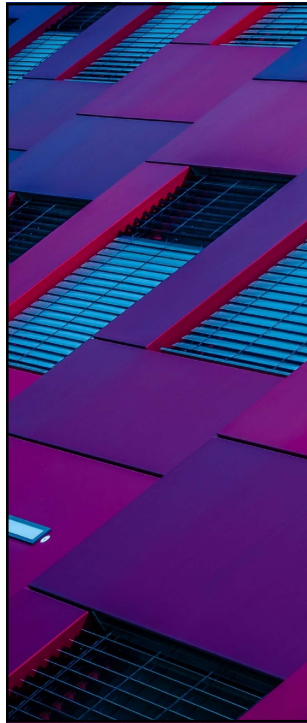
ANALYSIS

New Developments in Law Firms’ Obligations To Protect Against Data Breaches

In addition to a 2018 ABA ethics opinion which outlines when law firms are ethically obligated to notify clients of data breaches jeopardizing the security of their confidential information, the California Bar Association has handed down additional guidance on the subject, which is helpful to all law firms.

MAYER BROWN

24



ETHICAL OBLIGATIONS – CYBERSECURITY INCIDENTS

- July 2024, the New York City Bar Association's Professional Ethics Committee issued [Formal Opinion 2024-3: Ethical Obligations Relating to a Cybersecurity Incident](#). According to the NYCBA:
 - **Lawyers have an obligation of technological competence** under Rules 1.1 (Competence), 1.3 (Diligence), and 1.6 (Confidentiality of information) of the [New York Rules of Professional Conduct](#) **to take appropriate steps to protect clients' confidential data**
 - While lawyers may have statutory and regulatory notification requirements to which they are subject, they also have an ethical obligation under Rule 1.4 (Communication) **to promptly notify current clients in certain circumstances of the compromise of confidentiality or availability of client information** or if the firm will likely be unable to meet material obligations to the client;
 - There is **no ethical prohibition against, or requirement to, pay ransom to a cyber extortionist, and lawyers may not be candid with respect to certain material facts when negotiating with cyber-extortionists** in effort to protect or regain access to client information and firm systems;
 - **Lawyers can only disclose client confidential information to law enforcement or in connection with a government investigation of a cybersecurity event if permitted** by Rules 1.6 (Confidentiality), 1.8 (Current Clients: Specific Conflict of Interest) or 1.18 (Duties to Prospective Clients) and should be cognizant of potential risks to their clients of communicating with law enforcement or other government officials; and
 - Conflicts of interest may require lawyers not to advise a client in connection with the cybersecurity incident or to cease representing the client altogether in the event of a malpractice claim arising from the incident.

MAYER BROWN

25

ETHICAL OBLIGATIONS – ARTIFICIAL INTELLIGENCE TOOLS AND APPLICATIONS

- Under the Rules of Professional Conduct, a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.
- The duty of confidentiality extends to what client information a lawyer may share when using certain generative AI tools. Confidentiality concerns arise when:
 - Lawyers enter client information into AI engines. Generative AI systems can then share the information with third parties or use it for other purposes.
 - Even if a system does not share or use the inputted information, the AI system may lack adequate or reasonable security, thus increasing the risk that client information could be exposed or exploited.
 - Even in cases where an attorney is aware of the risks of disclosure to a third party, a paralegal or other attorney working at the direction of an attorney may rely on public AI tools and unwittingly expose privileged information.

Jan. 21, 2025, 4:30 AM EST

Careless Generative AI Use Puts Attorney-Client Privilege at Risk

Privileged communications are legally protected from disclosure, but they lose that protection if shared with someone else later. The advent of generative AI tools raises several unique questions about the concept of privilege for companies, which can take action now to mitigate risks.

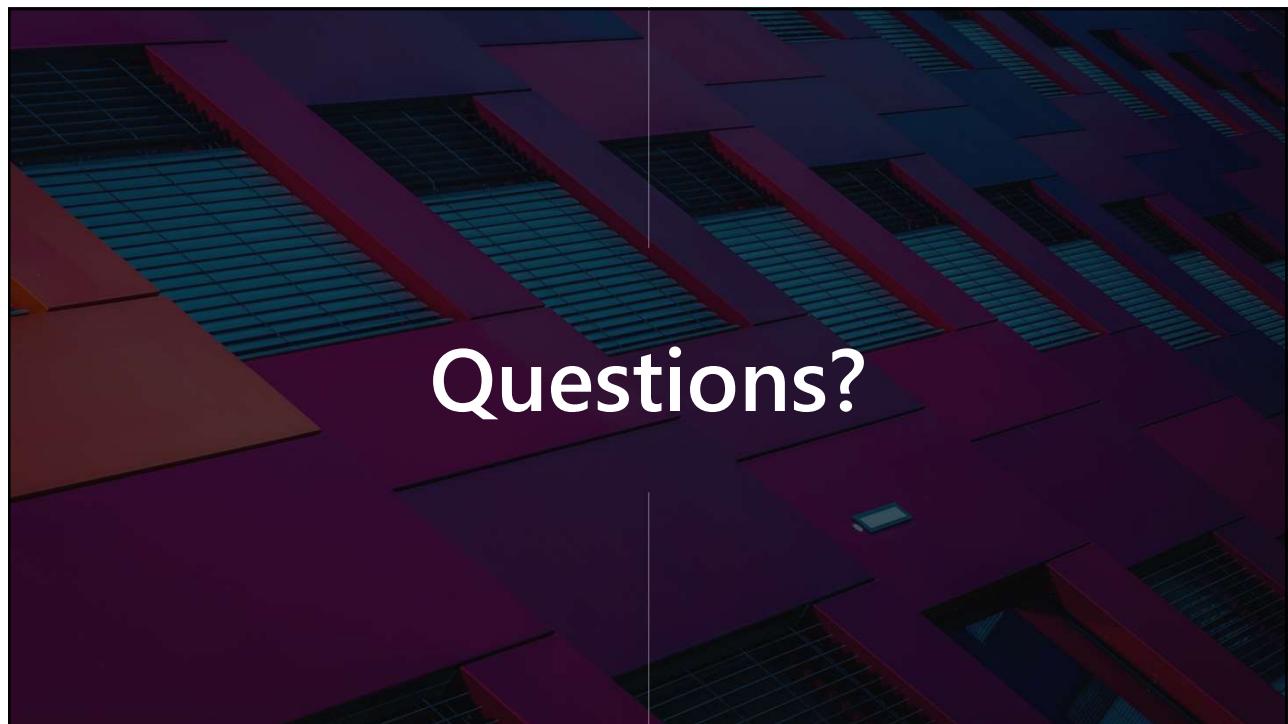
ANALYSIS

Legal Industry Players Missed a Microsoft AI Loophole That Could Expose Confidential Data

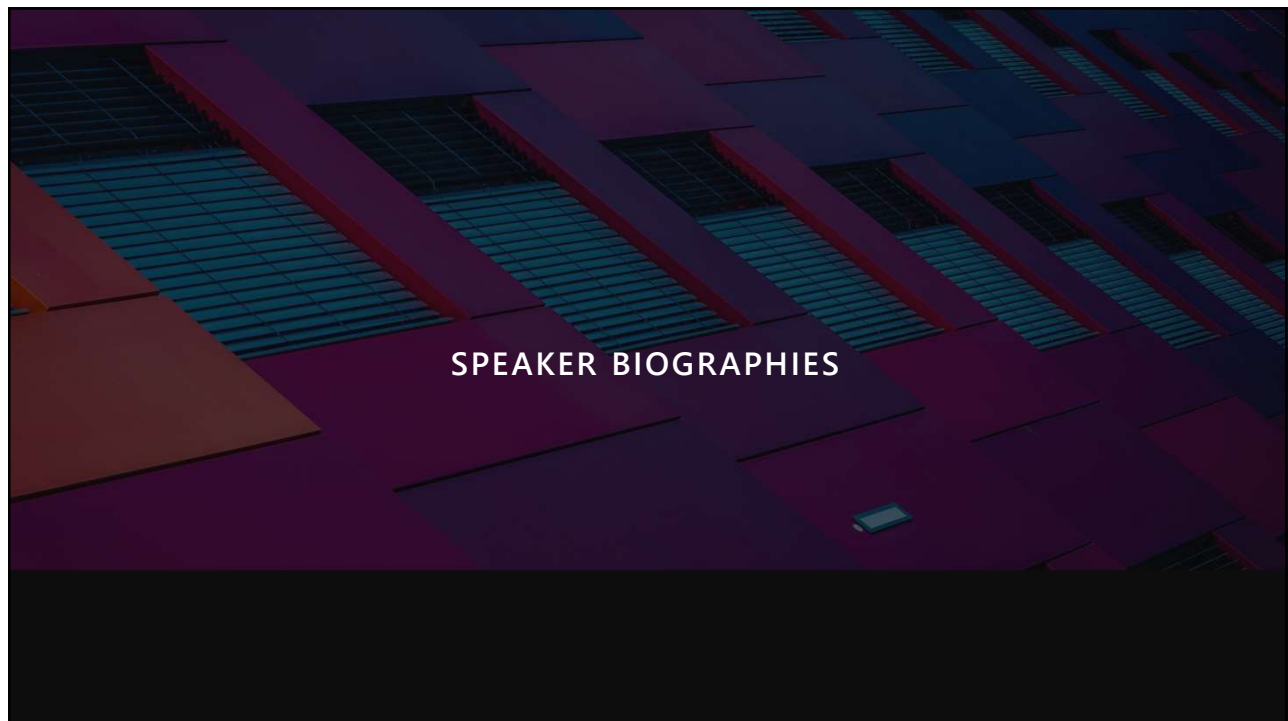
Sources told Legaltech News that several law firms and legal tech providers dove into integrations with Microsoft's Azure OpenAI Service without noticing the fine print that authorizes Microsoft employees to manually review certain prompts.

MAYER BROWN

26



27



28



GINA PARLOVECCHIO

MAYER BROWN

Gina Parlovecchio is a partner in Mayer Brown's New York office and serves as a co-chair of the Global Investigations & White Collar Defense practice. Previously, she was an Assistant United States Attorney (AUSA) in the US Attorney's Office for the Eastern District of New York (EDNY), where she served as the chief of the office's International Narcotics and Money Laundering Section (INMLS).

Gina represents individual and corporate clients in internal and government investigations and white collar criminal defense, with a particular focus advising on anti-money laundering (AML), securities fraud, bribery, corruption and healthcare fraud matters. Drawing upon her background prosecuting cross-border matters in the US and Central America, South America and Europe, Gina also advises clients on complex cross-border investigations. Gina's practice also focuses on complex civil litigation and trial practice. Her recent experience includes representing clients in trademark infringement matters, commercial disputes and pharmaceutical compliance related cases.

MAYER BROWN

29



JUSTIN HERRING

MAYER BROWN

Justin provides comprehensive representation and counseling on sophisticated cybersecurity matters, including global incident response, enforcement actions and related litigation, cyber monitorships and regulatory compliance. He also advises individuals and entities in the crypto and fintech sectors. Prior to joining Mayer Brown he was Executive Deputy Superintendent of the Cybersecurity Division at the New York State Department of Financial Services (NYDFS). His arrival underscores Mayer Brown's continued expansion of its cybersecurity and regulatory enforcement offerings and sustained growth in New York. At NYDFS, Justin served as the first leader of the agency's Cybersecurity Division, itself a first-of-its-kind unit at a financial services regulator. NYDFS issued the nation's first cybersecurity regulation for financial services, which has since become a model for other regulators such as the Federal Trade Commission, the Securities and Exchange Commission, and dozens of state banking and insurance regulators. Under Justin's leadership, NYDFS' Cybersecurity Division became a go-to source for guidance on novel and emerging cyber challenges. Among the influential regulation developed during his tenure was the creation of the nation's first cybersecurity regulation for financial services, and others adopted by the Federal Trade Commission and dozens of state banking and insurance regulators.

MAYER BROWN

30



JORDAN RAE KELLY

FTI CONSULTING

Jordan Rae Kelly is a Senior Managing Director and the Head of Cybersecurity for the Americas at FTI Consulting. Ms. Kelly has more than 15 years of experience coordinating incident response and managing cyber policy planning. Prior to joining FTI, she served as the Director for Cybersecurity Policy on the National Security Council at the White House and additionally, as Chief of Staff and Chief of Strategic Initiatives in the Federal Bureau of Investigation's (FBI) Cyber Division. Ms. Kelly advises clients on a broad range of cybersecurity and data privacy matters involving breaches, insider threats, intellectual property, crisis communications, vendor management, compliance, regulation, risk management, and forensic investigations.

MAYER BROWN

31



ALEXANDER MINDLIN

EASTERN DISTRICT OF NEW YORK

Alexander Mindlin is an Assistant United States Attorney for the Eastern District of New York, where he serves as a Deputy Chief for the Office's National Security and Cybercrime Section. From 2022 to 2024, he served on the Justice Department's National Cryptocurrency Enforcement Team, where he focused on illicit virtual asset exchanges, mixing services, and DeFi platforms. A longtime cybercrime prosecutor, he has investigated ransomware coders, intrusions into government and private networks, banking hacks, cyber-enabled securities fraud, illegal export of sensitive electronics, and large-scale bot-enabled ad-tech fraud schemes. Prior to joining the office, Alex was an associate at Davis Polk & Wardwell LLP and served as a law clerk to the Honorable Reena Raggi, United States Court of Appeals for the Second Circuit. Alex received his J.D. from NYU School of Law and his A.B. from Harvard University.

MAYER BROWN

32

