# SEC, FINRA, and NFA Zero in on Cybersecurity

## How You Can Prepare

Aaron Tantleff
Technology Transactions & Outsourcing
Privacy, Security & Information Management
Intellectual Property
Partner, Foley & Lardner LLP
atantleff@foley.com
312.832.4367

FOLEY
FOLEY & LARDNER LLP





- Questions can be entered via the **Q&A widget** open on the left-hand side of your screen. We will address questions at the end of the program, time permitting.
- If you experience technical difficulties during the presentation, please visit the Webcast Help Guide by clicking on the **Help button** below the presentation window, which is designated with a question mark icon.
- The PowerPoint presentation will be available on our website at Foley.com in the next few days or you can get a copy of the slides in the **Resource List** widget.
- Foley will apply for CLE credit after the program. To be eligible for CLE, you will need to log into the On24 session and answer a polling question during the program. If you did not supply your CLE information upon registration, please e-mail it to Brook Radford at **bradford@foley.com.**
- NOTE: Those seeking **Kansas, New York & New Jersey CLE** credit are required to complete the Attorney Affirmation Form in addition to answering the polling question that will appear during the program. A 4-digit code will be announced during the presentation. Email the code and the form to **bradford@foley.com** immediately following the program.



FOLEY
FOLEY & LARDNER LLP

# How'd We Get Here

- "More than 9 in 10 financial services organizations—93%—have experienced an incident in which the adequacy of their online security was tested, based on polling data from Kaspersky Lab and B2B International. In fact, despite the frequency with which cyberattacks occur, 33% of businesses don't have the type of protection needed to keep private data safe."

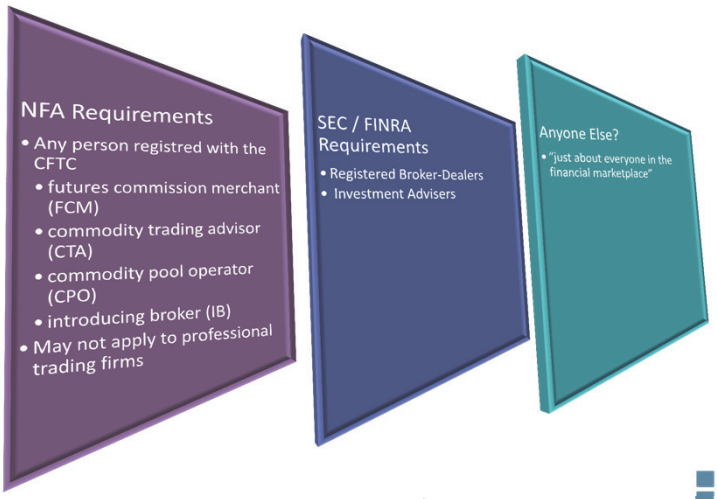
http://www.selective.com/fyi/Most-Financial-Firms-Affected-by-Potential-Data-Breach-This-Year-Survey-Reveals-950.aspx





FOLEY & LARDNER LLP

# Does This Apply To Me?








FOLEY & LARDNER LLP

# How'd We Get Here

- February 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity
  - Development of a voluntary, risk-based Cybersecurity Framework

Executive Order 13636: Cybersecurity Framework. The National Institute of Standards and Technology. November 12, 2013. http://www.nist.gov/cyberframework/





FOLEY & LARDNER LLP

# How'd We Get Here
# NIST Cybersecurity Framework

| | |
|---|---|
| Identify | • Asset Management (ID.AM)<br>• Business Environment (ID.BE)<br>• Governance (ID.GV)<br>• Risk Assessment (ID.RA)<br>• Risk Management Strategy (ID.RM) |
| Protect | • Access Control (PR.AC)<br>• Awareness and Training (PR.AT)<br>• Data Security (PR.DS)<br>• Information Protection Processes and Procedures (PR.IP)<br>• Maintenance (PR.MA)<br>• Protective Technology (PR.PT) |
| Detect | • Anomalies and Events (DE.AE)<br>• Security Continuous Monitoring (DE.CM)<br>• Detection Processes (DE.DP) |
| Respond | • Response Planning (RS.RP)<br>• Communications (RS.CO)<br>• Analysis (RS.AN)<br>• Mitigation (RS.MI)<br>• Improvements (RS.IM) |
| Recover | • Recovery Planning (RC.RP)<br>• Improvements (RC.IM)<br>• Communications (RC.CO) |

NIST Releases Cybersecurity Framework Version 1.0. The National Institute of Standards and Technology. February 12, 2014. http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm





FOLEY & LARDNER LLP

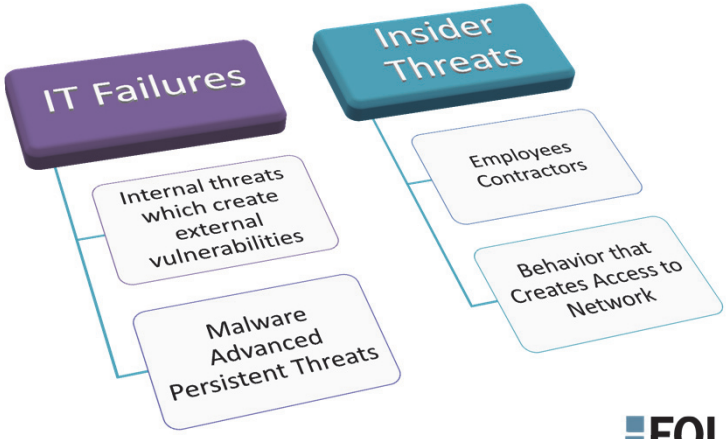
# How'd We Get Here

- April 15, 2014, SEC's Office of Compliance Inspections and Examinations (OCIE) announced its cybersecurity examination initiative
  - Assess cybersecurity preparedness
  - Gather information on practices and trends among registered firms
  - Result of a Cybersecurity Roundtable sponsored by the SEC in March 2014
- SEC Chair, Mary Jo White, expressed the importance of cybersecurity to the integrity of our market system and customer data protection
  - "cybersecurity has become one of the most significant issues affecting investors, corporate issuers, and financial institutions – really just about everyone in the financial marketplace."
- Commissioner Luis Aguilar
  - "it is not an overstatement to say that cybersecurity is one of the defining issues of our time."



FOLEY
FOLEY & LARDNER LLP

# SEC Cybersecurity Roundtable Key Takeaways






FOLEY
FOLEY & LARDNER LLP

# SEC Cybersecurity Roundtable Mitigation of Risk

## Identification of Data in Need of Protection

- Different types of information required different forms of protection... in some cases, multiple layers
- Firewalls, intrusion prevention, spam filter, anti-virus protection, vulnerability assessments, configuration management …

## Access Control

- Authentication
- Access Control

## Centralized Monitoring

- Monitor network activity and access to data



FOLEY
FOLEY & LARDNER LLP

# Cybersecurity Risk Alert

- February 2015, the SEC OCIE released the results of its cybersecurity examination via a Risk Alert
  - Summarized findings from the examination of more than 100 registered investment advisers and broker dealers
  - Most of the entities examined had directly or indirectly been the target of a cyber-attack



FOLEY
FOLEY & LARDNER LLP

# Cybersecurity Risk Alert

- Provides "guidance" to be used to assess a company's cybersecurity preparedness
- Included in the risk alert is a sample cybersecurity document
  - Tools to be used to assess an organization's preparedness for cybersecurity
  - Many of the same guidelines that drive the security industry
  - Addressing outside vendors
    - All third parties, including… law, accounting and marketing



FOLEY
FOLEY & LARDNER LLP

# Key Points From Risk Alert

- Almost 80% of investment advisers conduct periodic firm-wide risk assessments
  - Nearly 1/3 of IAs require vendors to conduct periodic firm-wide risk assessments where they have access to IA's network
- Fewer than 25% of IAs incorporate cybersecurity requirements into contracts with vendors and business partners
- Fewer than 15% of IAs maintain policies and procedures on information security training for vendors and business partners authorized to access their networks
- More than 70% of IAs have experienced cyber-related incidents
  - Majority were due to malware and fraudulent emails.



FOLEY
FOLEY & LARDNER LLP

# OCIE Examination Initiative

- Identify cybersecurity risks
- Establish cybersecurity policies, procedures and oversight processes
- Protect networks and information
- Identify and address risks associated with remote access to client information, funds transfer requests, and third-party vendors
- Detect and handle unauthorized activities and other cyberattacks

Cybersecurity Examination Sweep Summary. National Exam Program Risk Alert. The Office of Compliance Inspections and Examinations of the Securities and Exchange Commission. February 3, 2015. http://www.sec.gov/about/offices/ocie/cybersecurity- examination-sweep-summary.pdf





FOLEY & LARDNER LLP

# OCIE's Examination Initiative

- Continuation of previous cybersecurity exams and guidance
- Assess cybersecurity preparedness in the securities industry
- Ability to protect client information
- The 2015 Initiative will focus more on evaluating a firm's implementation of systems called for by the firm's policies or systems that OCIE believes the firm should have





FOLEY & LARDNER LLP

# OCIE Examination Initiative

- Assess cybersecurity preparedness
- OCIE will conduct examinations of more than 50 registered broker- dealers and registered investment advisers
- Focus on
  - Cybersecurity governance
  - Identification and assessment of cybersecurity risks
  - Protection of networks and information
  - Risks associated with remote customer access and funds transfer requests
  - Risks associated with vendors and other third parties
  - Detection of unauthorized activity
  - Experiences with certain cybersecurity threats

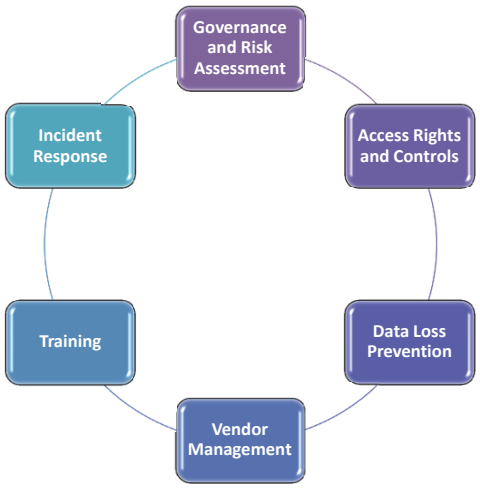
http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.





FOLEY & LARDNER LLP

# OCIE Examination Initiative








FOLEY & LARDNER LLP

# Governance and Risk Assessment

- Appropriate cybersecurity governance and risk assessment processes
  - technology, information access and vendor compliance
  - Prioritize remedial activities and initiatives
- Periodic evaluation of cybersecurity risks
- Tailored controls and risk assessment processes
- Internal investigation, decision-making and escalation within the organization to identify and manage cybersecurity risks
- Communication and involvement of senior management and boards of directors



FOLEY
FOLEY & LARDNER LLP

# Access Rights and Controls

- Implement basic controls to prevent unauthorized access to systems or information
  - protect information assets and technology, such as access management and control, data encryption and penetration testing
- Utiliztion of access control
- Review of access controls
  - Remote access, client logins, passwords, firm protocols to address client login problems, network segmentation and tiered access



FOLEY
FOLEY & LARDNER LLP

# Data Loss Prevention

- Patch management
- System configuration
- How one monitors the volume of content transferred outside of the company by its employees or through third parties
- How one monitors for potentially unauthorized data transfers
- How one verifies the authenticity of a client request to transfer funds



FOLEY
FOLEY & LARDNER LLP

# Vendor Management

- Third party vendor platforms
- Controls and processes related to vendor management
  - Due diligence
  - Oversight
  - Agreements
- Applicabilty of risk assessment to vendors
- Appropriate level of due diligence



FOLEY
FOLEY & LARDNER LLP

# Training

- Training tailored to specific job functions
  - Designed to encourage responsible employee and vendor behavior
  - Avoid unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured internet connection, or opening messages or downloading attachments from an unknown source
- Procedures for responding to cyber incidents under an incident response plan
  - Integration into regular personnel and vendor training



FOLEY
FOLEY & LARDNER LLP

# Incident Response

- Establish written policies, assigned roles, assessed system vulnerabilities and developed plans to address possible cybersecurity incidents
- Procedures and guidance for preparing for and responding to security incidents, including designation of an incident response team and roles and responsibilities
- Identifying and classifying data, assets, and services and determining appropriate protection from security incidents



FOLEY
FOLEY & LARDNER LLP

# Additional Risk Considerations

- Cyber Intelligence and Information Sharing
  - Responsibility should be assigned to one or more individuals for remaining current on the constantly evolving cyber threats and risks, and communicating those threats and risks throughout the organization
- Cyber-Risk Insurance
  - Recognizing that no firm will always maintain 100 percent security, firms should consider the use of cyber-risk insurance as another way of mitigating losses and exposure from security breaches and other cybersecurity incidents



FOLEY & LARDNER LLP

# OCIE Examination Initiative & Risk Alert Takaways

- OCIE expects each firm to have implemented more than a generic, cookie-cutter cybersecurity policy
  - Firms should actively analyze their particular risk profiles, and implement a policy specifically designed to address their relevant risks
  - Consider internal and external risks
  - Cybersecurity policies and procedures must be tailored to a firm's particular needs
  - At least an annual review and update, if applicable, of all policies
    - An effective plan involves the regular monitoring and analysis of potential risks including the risks arising from employees and vendors who inadvertently compromise the security of sensitive information
  - Document new risks to ensure the firm's program can keep pace with evolving threats
- Not sufficent to adopt a policy and not implement or monitor it
- An effective policy must include an incident response plan, including procedures to
  - Address what happens if data is compromised
  - Document the firm's response
  - Assess the extent of the impact on the firm and its clients
- Risk Alert highlights OCIE's concern that firms that fail to implement "basic controls" are at increased risk
  - Risl Alert seeks specific information regarding the technologies and technical processes firms have in place to protect customer information
  - OCIE examiners will be looking for evidence of a cybersecurity plan that addresses the risks based on a firm's own risk profile
  - The enumerated items of emphasis are not exclusive, and that examiners may select additional areas on which to focus, based on the risks identified in the course of the examinations



FOLEY & LARDNER LLP

# R.T. Jones

- On September 15, the U.S. Securities and Exchange Commission's (SEC's) Office of Compliance, Inspections and Examinations (OCIE), issued new guidance outlining areas of cybersecurity risk to be addressed by registered broker-dealers and investment advisers in their systems and procedures. The guidance, issued in the form of a "Risk Alert," sets forth examination priorities to be used by SEC examiners, in upcoming examinations of these firms. Just
- One week after the Risk Alert was issued, the SEC's Division of Enforcement filed its first enforcement action against St. Louis investment adviser R.T. Jones Capital Equities Management
- Violations surrounding an incident of hacking that exposed the firm's customers to risk of identity theft.
- While the case settled, it underscores the need for financial industry firms to have robust written procedures and systems to detect, prevent, and respond to instances of cybercrime and other breaches

Matter of R.T. Jones Capital Equities Management, Inc., Admin. Proc. File No. 3-16827, SEC Investment Advisers Act Release No. 4204 (Sept. 22, 2015)



FOLEY & LARDNER LLP

# R.T. Jones – The Case

- July 2013, R.T. Jones' third-party web server was attacked by an unauthorized intruder, whose identity was never discovered
  - Determined to originate from multiple IP addresses in China
  - Gained access and copy rights to nearly four years of PII of customers and third parties
  - Stored information was not encrypted
    - Firm restricted access to two individuals who held administrator status
- SEC alleged that "the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, was rendered vulnerable to theft."
- Upon learning of the breach, the firm promptly hired multiple cybersecurity consulting firms to investigate and assist the firm
  - Consultants could not assess the full extent of the breach because the log files had been destroyed in the attack by the intruder
  - Another cybersecurity consultant unsuccessfully attempted to determine if any of the PII stored on the server had been accessed
- The firm provided notice of the breach to all individuals whose PII may have been compromised and offered to provide free identity monitoring services
  - However, after 2 years, no knowledge that any client has suffered financial harm stemming from the breach



FOLEY & LARDNER LLP

# R.T. Jones – The Charges

- Violations of Rule 30(a) of SEC Regulation S-P, 17 C.F.R. § 248.30(a), the "Safeguards Rule."
  - Every investment adviser registered with the Commission adopt policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.
  - In its 2005 amendments the Safeguards Rule, the SEC required that such policies and procedures be in writing
- The SEC alleged that R.T. Jones did not have written policies and procedures that were reasonably designed to safeguard its clients' PII
  - While the SEC acknowledged that the firm did have some written procedures for protecting its clients' information, such procedures did not include such items as:
    - Conducting periodic risk assessments
    - Employing a firewall to protect the web server on which client PII was stored
    - Encrypting client PII stored on that server
    - Lacked any written policies or procedures for responding to a cybersecurity incident



FOLEY & LARDNER LLP

# R.T. Jones – The Sanctions

- Censured
- Cease and Desist from future violations of Rule 30(a) or Regulation S-P
- Fine of $75,000

- Odd… SEC did not impose a requirement that the firm retain an independent compliance consultant to review the firm's procedures and recommend any necessary improvements



FOLEY & LARDNER LLP

# National Futures Association

- US Forex broker FXCM Inc (NYSE:FXCM) recently accounced that it was a victim of a criminal cybersecurity incident involving unauthorized access to customer information
  - Detected a small number of unauthorized wire transfers from accounts of its customers
  - All funds have been returned
  - Received an email from a hacker claiming to have unlawful access to customer information
  - Broker immediately notified the FBI of this threat



FOLEY & LARDNER LLP

# NFA's ISSP

- On October 23, 2015, the NFA adopted the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 (Information Systems Security Programs (ISSP)), also known as the Cybersecurity Interpretive Notice
  - Commodity Futures Trading Commission (CFTC) approved NFA's Interpretive Notice
  - Applies to all Members
    - futures commission merchants
    - swap dealers
    - major swap participants
    - introducing brokers
    - forex dealer members
    - commodity pool operators
    - commodity trading advisors
  - Requires NFA members to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems
    - Adopt and enforce an ISSP appropriate to its circumstances
  - Effective March 1, 2016

http://www.nfa.futures.org/news/newsNotice.asp?ArticleID=4649
http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9



FOLEY & LARDNER LLP

# NFA's ISSP

- The Notice is "consistent" with the cybersecurity guidance published by other financial regulators, including the April 2015 Guidance Update issued by the SEC's Division of Investment Management (IM Guidance Update).
  - As with the IM Guidance Update, the Notice leaves "the exact form of an ISSP up to each Member . . . ."
  - The Notice is more detailed than the IM Guidance Update
  - NFA describes the required ISSP for its Members using different language, and therefore, asset managers and their affiliates that are NFA Members will need to review the Notice
    - Determine whether their current cybersecurity programs adequately address the guidelines
    - Take any necessary actions to implement appropriate ISSPs by the effective date



FOLEY
FOLEY & LARDNER LLP

# NFA's ISSP

- Written ISSPs should contain:
  - A security and risk analysis
  - A description of the safeguards against identified system threats and vulnerabilities
  - The process used to evaluate the nature of a detected security event, understand its potential impact, and take appropriate measures to contain and mitigate the breach
  - A description of the Member's ongoing education and training related to information systems security for all appropriate personnel
- ISSP review and training
  - ISSP must be approved within Member firms by an executive-level official and should be reviewed at least once a year
  - NFA members should provide their employees cybersecurity training
  - Programs must address risks posed by critical third-party service providers



FOLEY
FOLEY & LARDNER LLP

# NFA's ISSP - Guidelines

| | |
|---|---|
| Written Program | • "[e]ach Member firm must adopt and enforce a written ISSP reasonably designed to provide safeguards, appropriate to the Member's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities, to protect against security threats or hazards to their technology systems." In addition, the ISSP must be approved in writing by an executive-level official. If applicable, the Member's management should periodically provide information about the ISSP to the Member's governing body or its delegate, so it can "monitor the Member's information security efforts." |
| Security / Risk Analysis | • "a supervisory obligation to assess and prioritize the risks associated with the use of information technology systems."<br>• "maintain an inventory of critical information on technology hardware with network connectivity, data transmission or data storage capability and an inventory of critical software . . . ."<br>• identify and assess significant threats to "at-risk data" and "electronic infrastructure" and threats posed by third-party service providers<br>• "estimate the severity of potential threats, perform a vulnerability analysis, and decide how to manage the risks of these threats"<br>• consider past security incidents at the firm and "known threats identified by the firm's critical third-party service providers, the industry or other organizations" |
| Deployment of Protective Measures Against the Identified Threats and Vulnerabilities | • "document and describe" the Member's "safeguards deployed in light of identified and prioritized threats and vulnerabilities" and procedures "to detect potential threats." |
| Response and Recovery from Events that Threaten the Security of the Electronic Systems | • "should create an incident response plan to provide a framework to manage detected security events or incidents, analyze their potential impact and take appropriate measures to contain and mitigate their threat." Further, an "ISSP should contain . . . procedures to restore compromised systems and data, communicate with appropriate stakeholders and regulatory authorities and incorporate lessons learned . . . ." |
| Employee Training | • "a description of the Member's ongoing education and training relating to information security for all appropriate personnel." Training should be conducted upon hiring, as well as periodically throughout employment, and should be appropriately tailored to the particular firm.<br>• Training topics may include "social engineering tactics" and "other general threats posed for system compromise and data loss." |



FOLEY & LARDNER LLP

# NFA's ISSP

- Resources
  - National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)
  - Five general categories:
    - Identification of threats and vulnerabilities
    - Deployment of protective measures against the identified threats and vulnerabilities
    - Detection of threats in a timely manner
    - Response to events that threaten the security of the electronic systems
    - Recovery from the events



FOLEY & LARDNER LLP

# NFA's ISSP

- Examples of ISSP safeguards to be implemented:
  - Protecting the Member's physical facility against unauthorized intrusion by imposing appropriate restrictions on access to the facility and protections against the theft of equipment;
  - Establishing appropriate identity and access controls to a Member's systems and data, including media upon which information is stored;
  - Using complex passwords and changing them periodically;
  - Using and maintaining up-to-date firewall, and anti-virus and anti-malware software to protect against threats posed by hackers;
  - Using supported and trusted software or, alternatively, implementing appropriate controls regarding the use of unsupported software;
  - Preventing the use of unauthorized software through the use of application whitelists;
  - Using automatic software updating functionality or, alternatively, manually monitoring the availability of software updates, installing updates, and spot-checking to ensure that updates are applied when necessary;
  - Using supported and current operating systems or, alternatively, implementing appropriate controls regarding the use of unsupported operating systems;
  - Regularly backing up systems and data as part of a sustainable disaster recovery and business continuity plan;
  - Deploying encryption software to protect the data on equipment in the event of theft or loss of the equipment;
  - Using network segmentation and network access controls;
  - Using secure software development practices if the Member develops its own software;
  - Using web-filtering technology to block access to inappropriate or malicious websites;
  - Encrypting data in motion, (e.g. encrypting email attachments containing customer information or other sensitive information), to reduce the risk of unauthorized interception; and
  - Ensuring that mobile devices are subject to similar applicable safeguards.



FOLEY
FOLEY & LARDNER LLP

# What Does the Future Hold?

- Cybersecurity regulators are watching closely
  - SEC, FINRA, the Federal Trade Commission, Federal Financial Institutions Examination Council, Federal Communications Commission, and others…
- OCIE has issued two rounds of guidance
- OCIE and FINRA have already conducted one round of examinations
  - A second OCIE examination is pending



FOLEY
FOLEY & LARDNER LLP

# What Does the Future Hold?

- Findings from the second OCIE Examination Initiative are likely to result in significant compliance deficiencies and, potentially, enforcement actions
  - Expect another OCIE Risk Alert highlighting the SEC staff's observations.
- Now's a good a time as any to review previous guidance and perform a gap analysis
  - If you find a gap… fill it!



FOLEY
FOLEY & LARDNER LLP

# Contact and Questions

Aaron Tantleff
Technology Transactions & Outsourcing / Intellectual Property
Privacy, Security & Information Management

Foley & Lardner LLP
321 North Clark Street, Suite 2800
Chicago, IL 60654

Partner
312 832 4367
atantleff@foley.com


FOLEY
FOLEY & LARDNER LLP