Financial Regulations, Enforcement & Cybersecurity

Elizabeth P. Gray
James R. Burns
Norman C. Bay
Neal E. Kumar
Katherine Doty Hanniford

September 14, 2017

Administrative Items

The webinar will be recorded and posted to the FIA website following the conclusion of the live webinar.

A question and answer period will conclude the presentation.

- Please use the “question” function on your webinar control panel to ask a question to the moderator or speakers. Questions will be answered at the conclusion of the webinar.

CLE certificates will be emailed shortly after conclusion of the webinar.

Upcoming Webinars and Events

MiFID II: What Are We Waiting For?
September 20, 2017 | 10:00 AM – 11:00 AM EDT| Webinar

A CFTC Enforcement Refresher and Overview of Cooperation Credit
October 4, 2017 | 10:00 AM – 11:00 AM EDT | Webinar

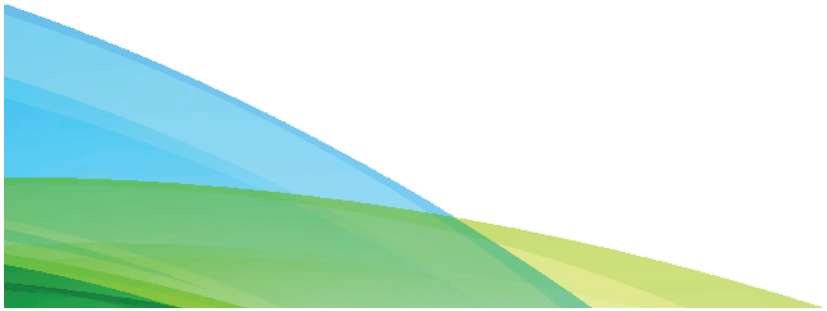
33rd Annual Futures & Options Expo
October 17-19, 2017| Hilton Chicago| Chicago, IL
*CLE offered for select sessions on Wednesday, October 18

Learn more and register at
FIA.org/events

FIA

Emergence of Cybersecurity as a Regulatory and Enforcement Priority Impacting Financial Services Firms

- Cybersecurity will be a top priority for financial regulators in 2017
  - SEC, CFTC, Treasury, FINRA and States
- Treasury Secretary Mnuchin: Regulatory agencies should focus on incorporating cybersecurity in all oversight responsibilities (March 17, 2017)
- These programs will include cybersecurity-related regulations, examinations and enforcement
  - Many regulations and enforcement regimes
  - Harmonization not yet a reality
- Across regulators, senior management and corporate boards will be expected to embrace cybersecurity as an enterprise risk and to implement a well tested and evolving cybersecurity program



FIA

Managing Cyber Risk - More Compelling Each Day

More Attacks…

More Targets…

More government oversight…

MORE RISK & LIABILITY

Examples Highlight the Real Risks

Equifax – 2017

- ? ? ?

Petya Ransomware – 2017

- $100s Millions in Lost Revenues and Costs
- Millions more in lost goodwill, reputation
- Regulatory fines coming?

WannaCry Ransomware – 2017

- Estimates of ~$4 billion in financial, economic losses

Yahoo! Breaches – 2016

- $350M Loss in Company Value
- SEC, FTC, and others Investigating
- ~20 Class Actions

Anthem Breach – 2015

- ~$115M class action settlement
- ~$100M in response/recovery costs

Don't forget about Target, Sony, Home Depot…

Navigate the Cybersecurity Regulatory Maze

Federal:

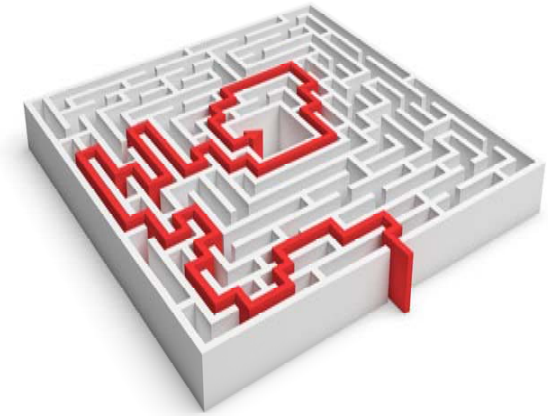
- Commodity Exchange Act
- Securities Exchange Act of 1934
- Federal Trade Commission Act
- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act

State:

- New York DFS Cyber Rules
- State Breach Notification Laws (48 States!)

International:

- EU's General Data Protection Regulation
- China's Cybersecurity Law



This is just a sample of the laws and regulations that implicate cybersecurity and privacy issues.

Commodity Futures Trading Commission Regulations

Cybersecurity as a Key CFTC Issue

- Chairman Giancarlo: "Cyber risk is undoubtedly the number one threat to 21st century financial markets." Sept. 21, 2016
  - "I favor bottom-up principles-based market solutions. I believe that markets themselves, reflecting the myriad actions of the broad sway of participants, remain the most efficient agents of change known to humankind." Oct. 26, 2015
- Commissioner Behnam: During the confirmation process, referenced the "need for strong enforcement" along with his concern regarding "cyber-security threats" in a hearing before the Senate Agricultural Committee. July 27, 2017
- Commissioner Bowen: "[W]hile I believe our current rules are strong, they could be improved… Because of the interconnected nature of our financial system, our cybersecurity protections are only as strong as our weakest link." Mar. 14, 2017

Overview of Major Rules

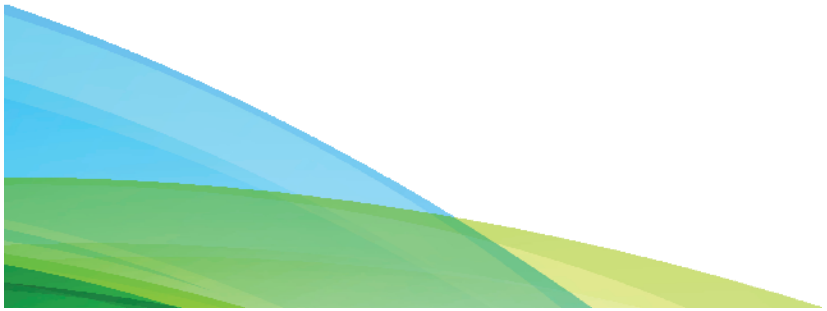
- System Safeguards for Market Infrastructure:
  - Designated contract markets (DCM) (CFTC Rule 38.1051)
  - Swap execution facilities (SEF) (CFTC Rule 37.1401)
  - Swap data repositories (SDR) (CFTC Rule 39.24)
  - Derivatives clearing organizations (DCO) (CFTC Rule 39.18 & 39.34)
- System safeguards for intermediaries and advisors (CFTC Rule 160.30):
  - Futures commission merchants (FCM)
  - Swap Dealers (SD)
  - Commodity trading advisors (CTA)
  - Commodity pool operator (CPO)
  - Introducing broker (IB)
- National Futures Association Interpretation 9070 (Aug. 20, 2015)

System Safeguards for Market Infrastructure

- In September of 2016, the CFTC adopted final rules clarifying certain rules applicable to market infrastructure and establishing new testing requirements
  - System Safeguard Testing Requirements, 81 Fed. Reg. 64272 (Sept. 19, 2016)
  - System Safeguard Testing Requirements for Derivatives Clearing Organizations, 81 Fed. Reg. 64322 (Sep. 19, 2016)
- "Detect, contain, respond to, and recover from cyber attacks"
- Requirement to follow "generally accepted standards and best practices"

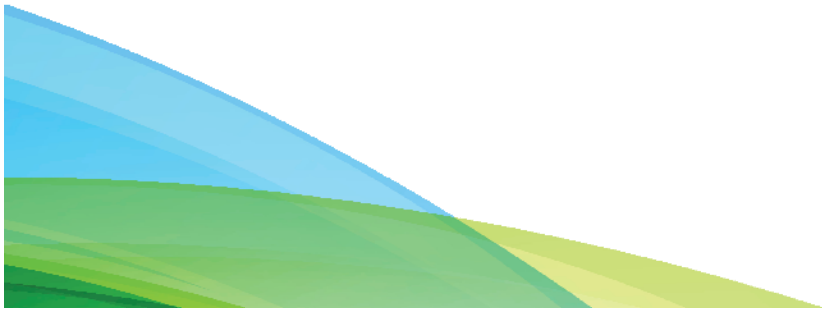
Market Infrastructure: Risk Analysis and Oversight

- Enterprise risk management and governance
- Information security
- Business Continuity Disaster Recovery (BCDR) planning and resources
- Capacity and performance planning
- Systems operations
- Systems development and quality assurance
- Physical security and environmental controls



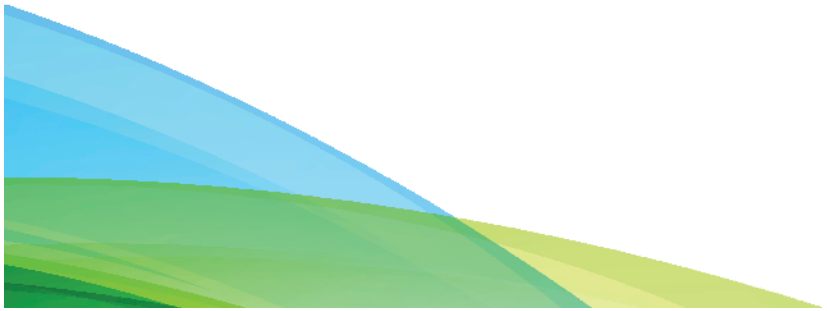
Market Infrastructure: New Testing Requirements

- Vulnerability Testing
  - At least quarterly for SDRs and covered DCMs, otherwise as frequent as risk analysis indicates
  - Independent contractors or independent employees
  - First compliance date: March 18, 2017
- External Penetration Testing
  - At least annually for SDRs and covered DCMs, otherwise as frequent as risk analysis indicates
  - SDRs and Covered DCMs must engage independent contractors to perform testing, for all others, independent contractors or independent employees
  - First compliance date: September 19, 2017



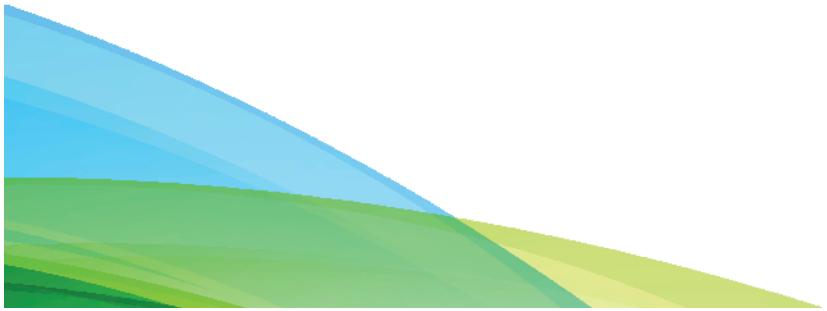
Market Infrastructure: New Testing Requirements *(cont'd)*

- Internal Penetration Testing
  - At least quarterly for SDRs and covered DCMs, otherwise as frequent as risk analysis indicates
  - Independent contractors or independent employees
  - First compliance date: September 19, 2017
- Controls Testing
  - SDRs and Covered DCMs: (1) independent contractors to test key controls at least every three years; and (2) independent contractors or independent employees to test non-key controls as frequent as risk analysis indicates
  - All other entities may use independent contractors or independent employees to must perform controls testing as frequent as risk analysis indicates
  - First compliance date: September 19, 2017 and September 19, 2019 (key controls)



Market Infrastructure: New Testing Requirements *(cont'd)*

- Security Incident Response Plan (SIRP)
  - At least annual testing for SDRs and covered DCMs , for all other entities, as frequent as risk analysis indicates
  - Independent contractors or employees
  - First compliance date: March 18, 2017
- Enterprise Technology Risk Assessment
  - At least annual testing for covered DCMs and SDRs, for all other entities, as frequent as risk analysis indicates
  - First compliance date: September 19, 2017



Market Infrastructure: Review – Reporting – Remediation

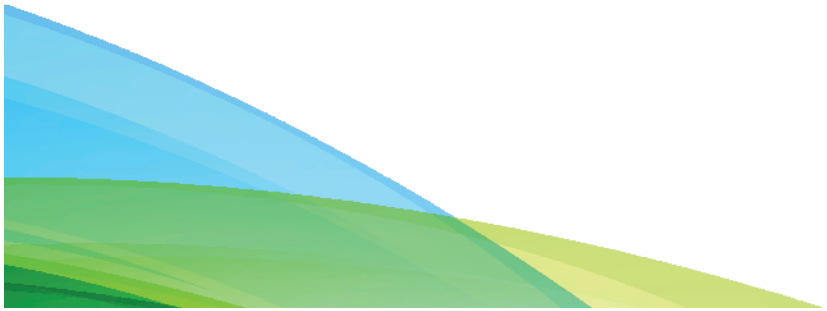
- Senior management and the board of directors of a SDR, SEF, or DCM shall receive and review reports setting forth the results of the assessment and testing required by the rule
- Level of detailed provided should be sufficient to provide senior management and board with the ability to conduct effective, knowledgeable oversight of cybersecurity
- Identify and document the vulnerabilities and deficiencies revealed by the testing
- Conduct and document an appropriate analysis of the risks presented in order to determine whether to remediate or accept each risk

System Safeguards for Intermediaries and Advisors

- Part 160 of the CFTC regulations establish privacy protections for "individuals who obtain financial products or services primarily for personal, family, or household purposes from [FCMs, RFEDs, CTAs, CPOs, IBs, MSPs, or SDs]"
- Privacy notices with model form available
  - Initial, annual, and revised privacy notice detailing privacy policies and procedures
  - Opt out notices
- Limits on disclosure of customer information to nonaffiliated third parties

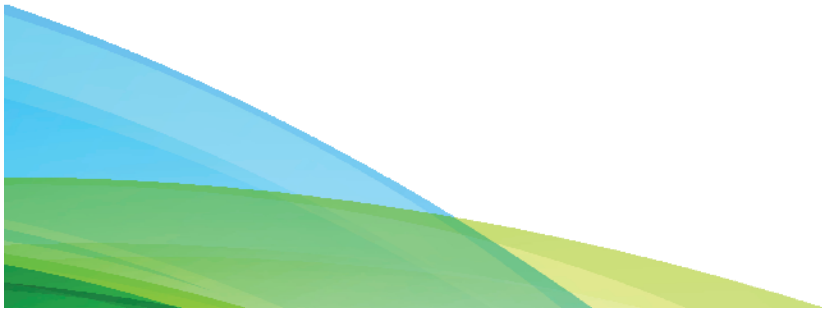
Privacy Policies and Procedures

- Rule 160.30 obligates covered entities to establish policies and procedures that address safeguards for the protection of customer information
- On June 29, 2009, Interbank FX, a registered FCM, paid a $200,000 penalty to settle changes for alleged failures in its privacy policies and procedures
  - IT placed files containing personal identifying information (e.g., bank account numbers, social security numbers etc.) of 13,000 customers or potential customers on a generally accessible website
  - Information accessible for approximately 1 year
- On February 26, 2014, the CFTC's Division of Swap Dealer and Intermediary Oversight published "recommended best practices" concerning security safeguards to implement under Part 160



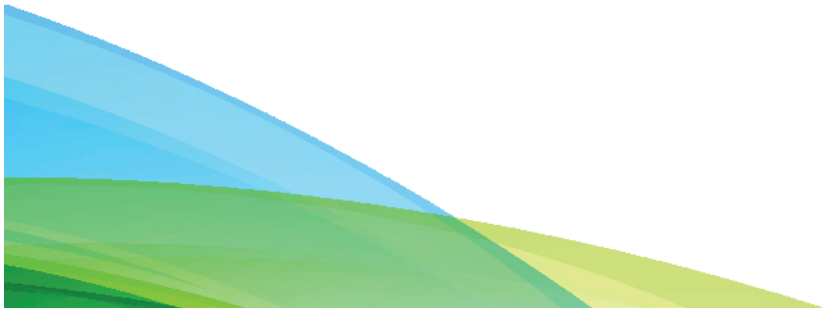
CFTC Staff Advisory 14-21 (Feb. 26, 2014): Best Practices for Part 160

- Designate employee with privacy and security management oversight
- Identify, in writing, all internal and external risks to security
- Design safeguards to control the identified risks
- Training
- Regularly test safeguards, policies, and procedures
- Engage independent party to test and monitor safeguards
- Oversee service providers with access to PII
- Regularly evaluate and adjust the program
- Design policies and procedures for incident response
- Annual assessment for board of directors



SD and FCM Risk Management Program

- Pursuant to CFTC Rule 23.600(c)(4)(i), an SD's risk management program must address operational risk and take into account ("among other things"):
  - Secure and reliable operating and information systems with adequate, scalable capacity, and independence from the business trading unit
  - Safeguards to detect, identify, and promptly correct deficiencies in operating and information systems
  - Reconciliation of all data and information in operating and information systems
- Pursuant to CFTC Rule 1.11(e)(3)(ii), an FCM's risk management program must address operational risk



National Futures Association Cybersecurity Initiatives

NFA Interpretive Notice 9070 (Mar. 1, 2016)

- On March 1, 2016, NFA issued an Interpretive Notice 9070 detailing information security practices that member firms should adopt and tailor to their particular business
- NFA issued the interpretation to provide specific guidance on acceptable standards for supervisory procedures for NFA compliance rules that address supervisory obligations:
  - FCMs, CTAs, and IBs (NFA Rule 2-9)
  - RFEDs (NFA Rule 2-36)
  - SDs and MSPs (NFA Rule 2-49)
- Members should have supervisory practices in place reasonably designed to diligently supervise the risks of unauthorized access or attack of their information technology systems, including the ability to respond appropriately
- NFA Interpretative Notice 9070 was designed to establish general requirements for an information systems security program (ISSP), but leave the exact form of an ISSP up to members
- The ISSP may be part of a broader program for a corporate group, but must comply with NFA rules

NFA Information Security Systems Program

- Establish a governance framework that supports informed decision making and escalation of security risks
- Written ISSP reasonably designed to provide safeguards to protect against security threats or hazards to technology systems
  - ISSP approved, in writing, by the CEO, CTO, or other relevant official
  - Senior management should provide sufficient information about ISSP to board of directors or similar governing body (or relevant board committee)
  - Firms should consider best practices promulgated by: the SANS Institute, Open Web Application Security Project, ISACA Control Objectives for Information and Related Technology (COBIT), and/or the National Institute of Standards and Technology (NIST) (NIST cybersecurity framework)
- Assess and prioritize the risks associated with the use of information technology systems (security risk analysis)
  - Inventory of critical systems
  - Identify internal and external vulnerabilities

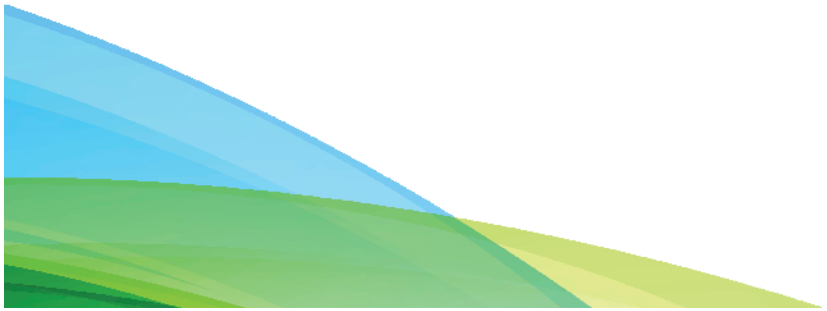
NFA Information Security Systems Program *(cont'd)*

- Deploy protective measures in light of the risks identified
- Create an incident response plan to provide a framework to manage detected security incidents
- Provide education and training for appropriate personnel
- Review effectiveness of ISSP (at least once every 12 months)
- Assess and monitor the risks posed by third party service providers
- Retain records related to the adoption and implementation of an ISSP

The Securities and Exchange Commission's Cybersecurity Initiatives

SEC Expectations concerning Cybersecurity

- SEC has implemented cybersecurity regulations and examinations, and initiated enforcement actions enforcing those rules
  - Focus has been on broker-dealers and investment advisers
- SEC Chair Jay Clayton
  - "The SEC is […] working closely with fellow financial regulators to improve our ability to receive critical information and alerts and react to cyber threats. . . . Public companies have a clear obligation to disclose material information about cyber risks and cyber events. I expect them to take this requirement seriously. . . . [T]he SEC needs to have a broad perspective and bring proportionality to this area that affects not only investors, companies, and our markets , but our national security and our future."
- First series of cybersecurity-related examinations began in 2014
  - SEC is bringing back surprise examinations
  - OCIE refers significant deficiencies to SEC Division of Enforcement for further investigation



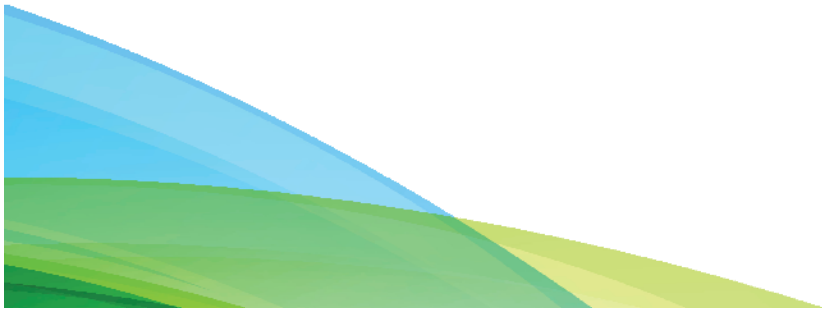
FIA

What to Expect Under SEC Chair Jay Clayton?

- SEC will expect public companies and regulated entities (investment advisers and broker-dealers) to have comprehensive and appropriately evolving cybersecurity programs
- Increased SEC focus on adequacy and accuracy of disclosures by public companies and regulated entities about their cybersecurity programs, cyber threats and related impact on those companies

SEC Enforcement of Existing Regulations

- The SEC has brought multiple enforcement actions for failure to protect customer data, demonstrating its willingness to pursue punitive measures to ensure compliance with the Safeguards Rule of Regulation S-P.
  - These actions signal that any informal grace period for implementing effective cybersecurity protocols, consistent with SEC guidance, may have expired
  - In announcing a recent settlement, former SEC Enforcement Director Andrew Ceresney reiterated that “the dangers and impact of cyber breaches” make data security “a critically important aspect of investor protection.”

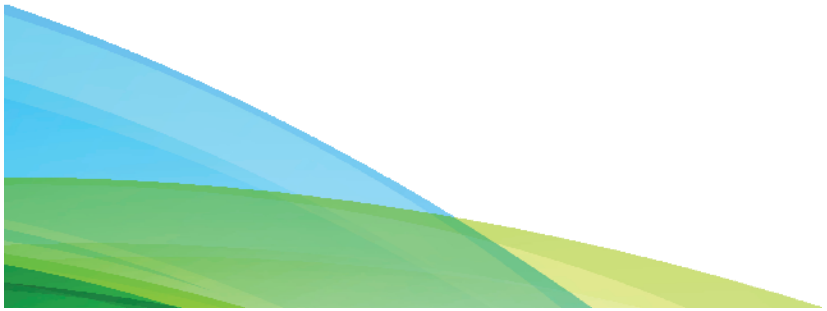


Regulation S-P

- Regulation S-P is designed to protect individual identifying information of "natural persons"
- Requires broker-dealers to adopt policies and procedures that: (i) "address administrative, technical, and physical safeguards for the protection of customer records and information;" and (ii) are reasonably designed to
  - insure the security and confidentiality of customer records and information;
  - protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
  - protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.
- Regulation S-P also requires advisers to deliver an initial, revised and annual privacy notices to all natural person investors.
  - Private funds (as distinct from their advisers) must comply with the FTC and CFPB regulations and privacy framework. Generally, private funds can comply with these rules by adopting policies and procedures that are designed to comply with Regulation S-P.

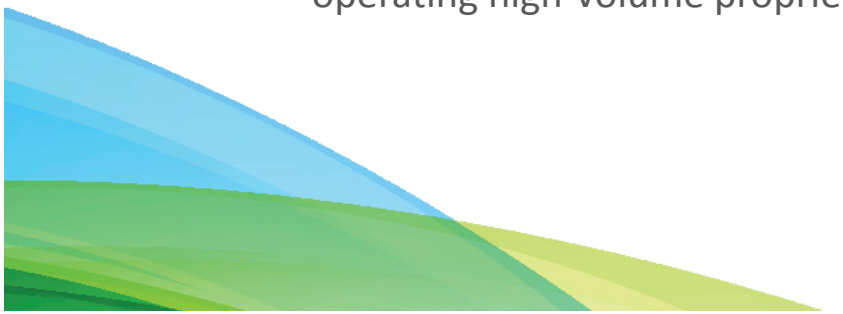
Regulation S-ID

- Regulation S-ID was adopted in April 2013 and is commonly referred to as the Identity Theft Red Flag Rule.
- These broker-dealers are required to develop, implement, and administer a written identity theft prevention program.
- The program must be designed to detect, prevent, and mitigate identity theft in connection with the opening of investor accounts and the administration of current accounts.
- Programs implemented to comply with Regulation S-ID must, among other requirements:
  - address training of employees to identify red flags;
  - ensure third-party service providers to covered accounts have their own reasonable red flags programs in place; and
  - provide for an annual review of the program.



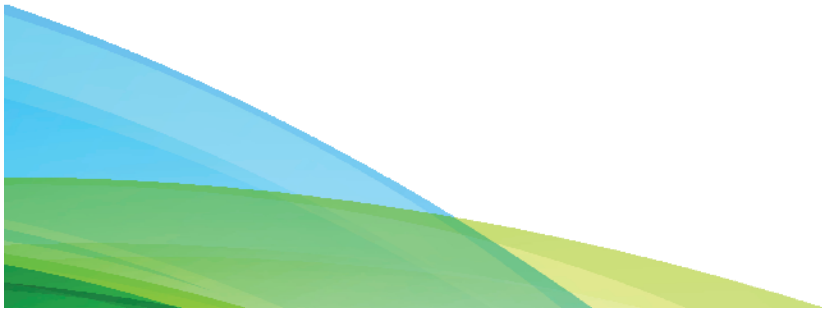
Regulation SCI

- Requires:
  - Policies and procedures to ensure the entity's systems can maintain its operational capabilities and promote fair and orderly markets, including, for example:
    - Business continuity and disaster recovery plans providing for next business day resumption of trading and two-hour resumption of certain "critical SCI systems" following a wide-scale disruption
    - Response plan to an "SCI Event"
  - Annual SCI compliance review
  - Quarterly notices to the SEC of systems changes
- Applies to national securities exchanges, higher-volume equity ATSs, FINRA, securities information processors, each registered and one exempt clearing agency, and the Municipal Securities Rulemaking Board
  - Does not apply to ATSs trading only fixed-income securities or broker-dealers operating high-volume proprietary trading platforms



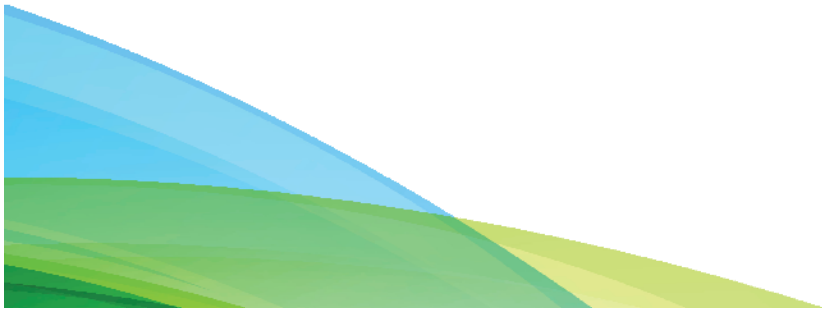
Business Continuity / Transition Planning Rule Proposal

- In late June 2016, the SEC proposed a new rule to address potential ramifications of a temporary or permanent interruption of a registered adviser's ability to provide advisory services.
- As proposed, the rule would require an adviser to:
  - Adopt and implement plans to ensure business continuity after a significant business disruption; and business transition in the event the adviser is unable to continue providing advisory services;
  - Conduct an annual review of those plans; and
  - Comply with corresponding recordkeeping plans.



Business Continuity / Transition Planning Rule Proposal *(cont'd)*

- In proposing this rule, the SEC is indicating that the efforts advisers have undertaken under the existing Rule 206(4)-7 are not sufficient.
- In the cybersecurity arena, the rule proposal emphasizes:
  - An adviser is expected "to prevent, detect and respond to cyber attacks"
  - Cybersecurity incidents may result in exposure to compliance and operational risks for an adviser.
  - Data protection, backup, and recovery plans should address both hard copy and electronic backup and focus on risks related to cyber-attacks.
- Notably, the SEC indicates in the proposing release that a violation of the rule, as proposed, would constitute an act of fraud.



SEC Cybersecurity Examination Initiative: 2015 – Second Round of SEC Examinations

- September 2015: OCIE published Risk Alert to provide additional information on areas of focus for its second round of cybersecurity examinations
  - General focus is on firms' ability to protect firm client information and on weaknesses in basic cybersecurity-related controls. OCIE specifically identified the following areas of focus:

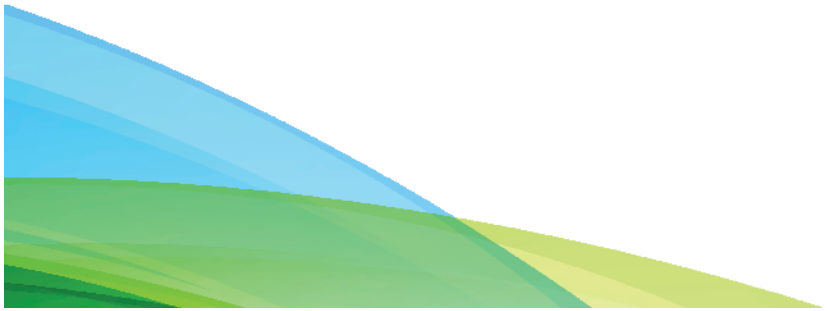
Governance and risk assessment processes	• **Periodic evaluations** • **Communications to and involvement of senior management and directors** • **Chief Information Security Officer**
Access rights and controls	• Basic controls to prevent unauthorized access to systems or information
Data loss prevention	• Controls in areas of patch management and system configuration • Transfers of content outside the firm • Monitoring procedures
Vendor management	• Due diligence as to vendor selection • Monitoring and oversight of vendors • Contract terms
Training	• Employees and vendors
Incident Response	• Plans to mitigate the effects of a cybersecurity incident • Information about actual cybersecurity incidents, including the extent of customer losses and remedial efforts

2017 Risk Alert

- OCIE issued a risk alert that identified certain cybersecurity program aspects that most examined firms had in common, signaling a certain level of maturation within the industry.
  - Critical risk assessments
  - Penetration testing and vulnerability analysis
  - Specific policies and procedures
  - Cybersecurity function with roles, responsibilities delineated and in writing.
  - Incident response plan, including ones for specific scenarios

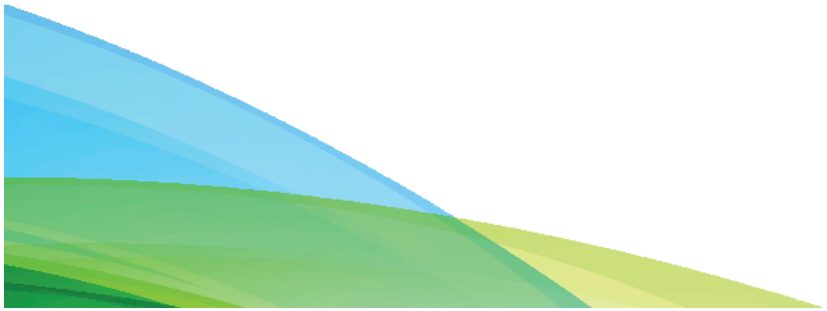
2017 Risk Alert

- OCIE also identified a number of shortcomings that it would like firms to consider in order to assess and improve cyber-related policies and procedures. Among these:
  - Are your policies and procedures sufficiently tailored to the firm's needs?
  - Do you actually do what your policies say you do? How do you ensure that?
  - How engaged is senior management?
  - How do you ensure timely remediation of high-risk vulnerabilities?



ICOs and Distributed Ledger Technology

- The SEC recently issued an investigative report on The DAO, a virtual organization, finding The DAO's "Initial Coin Offering" or "Token Sale" was subject to federal securities laws.
- The facts and circumstances of each ICO determine whether the virtual coins or tokens are securities. If so, they are subject to federal securities laws.
  - SEC Press Release: "[T]he federal securities laws apply to those who offer and sell securities in the United States, regardless of whether the issuing entity is a traditional company or a decentralized autonomous organization, regardless whether those securities are purchased using U.S. dollars or virtual currencies, and regardless of whether they are distributed in certificated form or through distributed ledger technology."
- Issuers of distributed ledger or block chain technology-based securities must register offers and sales of such securities unless a valid exemption applies.
  - Liability may extend to those participating in unregistered offerings and exchanges providing for trading these securities, unless an exemption applies.



FIA

Financial Industry Regulatory Authority (FINRA)

FINRA

- FINRA (Financial Industry Regulatory Authority) reviews a firm's ability to protect the confidentiality, integrity and availability of sensitive customer information. This includes reviewing each firm's compliance with SEC regulations, including:
  - Regulation S-P (17 CFR §248.30), which requires firms to adopt written policies and procedures to protect customer information against cyber-attacks and other forms of unauthorized access
  - Regulation S-ID (17 CFR §248.201-202), which outlines a firm's duties regarding the detection, prevention, and mitigation of identity theft
  - The Securities Exchange Act of 1934 (17 CFR §240.17a-4(f)), which requires firms to preserve electronically stored records in a non-rewriteable, non-erasable format.

FINRA *(cont'd)*

- In February 2015, FINRA published a report on Cybersecurity Practices ("FINRA Report"). The FINRA Report recommended firms organize their cybersecurity program along the following sections:
  - cybersecurity governance;
  - risk management;
  - cybersecurity risk assessment;
  - technical controls;
  - incident response planning;
  - vendor management;
  - staff training;
  - cyber intelligence and information sharing; and
  - cyber insurance.

FINRA *(cont'd)*

- In the FINRA Report, FINRA urges firms to report material cyber incidents that do not trigger a reporting obligation to their regulatory coordinator.
- FINRA also recommends firms use industry frameworks and standards in designing their cybersecurity program such as from NIST (National Institute of Standards and Technology).
- FINRA expects that firm management will make cybersecurity a priority and that it will devote sufficient resources both to understand the current and evolving cybersecurity threats to which the firm may reasonably expect to be exposed and to implement measures necessary to achieve the desired risk posture.
- FINRA also published a checklist for a small firm's cybersecurity program.

FINRA *(cont'd)*

- FINRA has also provided guidance as to what constitutes reasonable data security practices in the form of enforcement actions and other agency publications.
  - Lincoln Financial Securities Corporation ("LFS") – FINRA Letter of Acceptance, Waiver and Consent No. 2013035036601 (November 14, 2016) – FINRA alleged that LFS failed to ensure that the third-party vendor that configured the cloud-based server properly installed anti-virus software or data encryption. Insufficient data security policies and procedures regarding the storage of customer data on cloud servers. LFS did not adequately test and verify the security of information that continued to be stored on cloud-based servers, and could not tell whether a computer server was breached. Fine of $650,000 and undertaking to review written supervisory procedures and to implement revisions that are reasonably designed to achieve compliance with the Safeguarding Rule.

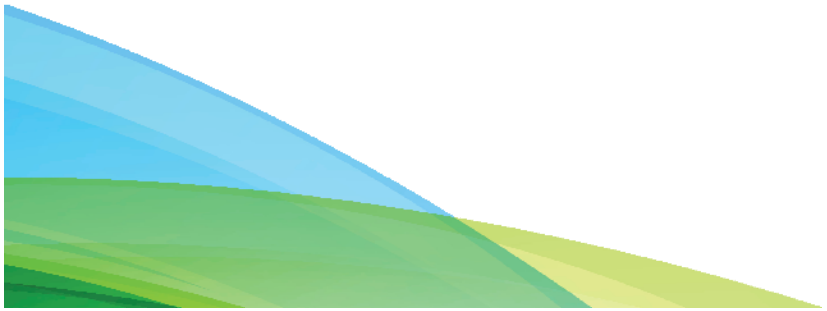
FINRA *(cont'd)*

- American Enterprise Investment Services Inc. and Ameriprise Financial Services – Financial Industry Regulatory Authority Letter of Acceptance, Waiver and Consent No. 2010025157301 (Mar. 1, 2013) – FINRA alleged that American and Ameriprise did not adequately protect customer records and information by failing to prevent brokers who had been terminated from continuing to access the firm's computer system. American and Ameriprise agreed to a censure and a joint and several fine of $750,000.
- Wells Investment Securities Inc., Letter of Acceptance, Waiver and Consent No. 2009019893801 (Nov. 21, 2011) – FINRA's investigation also found that Wells failed to have supervisory procedures in place to ensure that sensitive customer and proprietary information stored on laptops were being adequately safeguarded by appropriate encryption technology. Wells was fined $300,000 for its data security lapses among other compliance issues.

State Data Security Laws – Massachusetts and New York

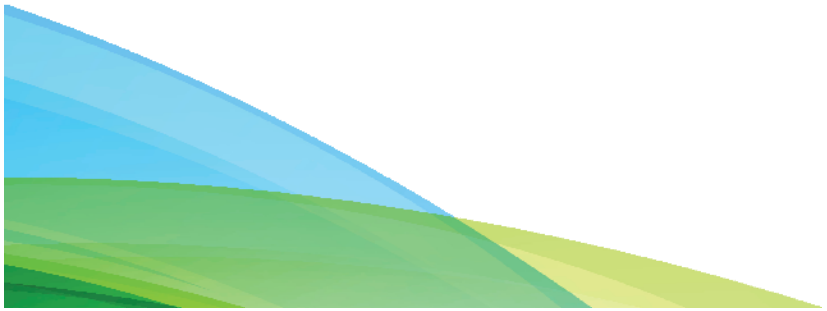
State Data Security Laws - Massachusetts

- The Massachusetts data protection regulation, Standards for the Protection of Personal Information of Residents of the Commonwealth ("MA Data Security Regs"), 201 C.M.R. 17, is the most detailed information data security rule in the United States.
- The cornerstone of the MA Data Security Regs is the development of a comprehensive information security policy that must be tailored to the size, scope and resources of the business, and to the amount of PI to be safeguarded.
- The MA Data Security Regs apply to any business that receives, stores or maintains a combination of certain personally identifying information of Massachusetts residents that is not publicly available.



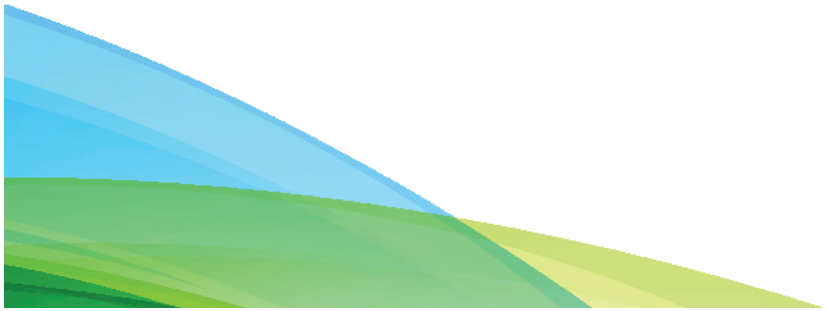
State Data Security Laws – Massachusetts *(cont'd)*

- Some of the requirements include:
  - Designating one or more employees to maintain the policy;
  - Ongoing employee training and discipline of employees who violate the policy
  - Monitoring employees and computer systems;
  - **Oversight of service providers through contract provision requirements and due diligence in selecting service providers;**
  - Password protection and/or two-factor authentication for computer systems;
  - Encryption of Personal Information that is transmitted over public networks or wirelessly and encryption of Personal Information stored on laptops and other portable devices to the extant technically feasible;
  - Use of software that employs malware protection and reasonably up-to-date patches and virus definitions, and institute procedures for staying current on security updates.



State Data Security Laws – Massachusetts *(cont'd)*

- The MA Data Security Regs defines PI more narrowly than the GLB Act to include a Massachusetts resident's first and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to the resident's financial account.
- Penalties for non-compliance could be up to $5,000 per violation and what constitutes a violation could be broadly defined. The MA Attorney General could seek other relief that may be appropriate.
- In addition, failure to properly dispose PI may result in penalties of $100 per person affected with a maximum cap of $50,000 for each instance of improper data disposal.



State Data Security Laws – Massachusetts *(cont'd)*

- On January 7, 2013, Suffolk Superior Court approved consent judgments involving four pathology groups where it was agreed that they would collectively pay $140,000 for violations of the MA Data Security Regs, by among of things, for not taking reasonable steps to select and retain a service provider that would maintain appropriate security measures to protect PI when a medical billing company hired as a service provider improperly disposed of PI at a public dump. Complaint Sections 1-8, Massachusetts v. Gagnon, No. 12-4568 (Mass. Super. Ct. Dec. 20, 2012).

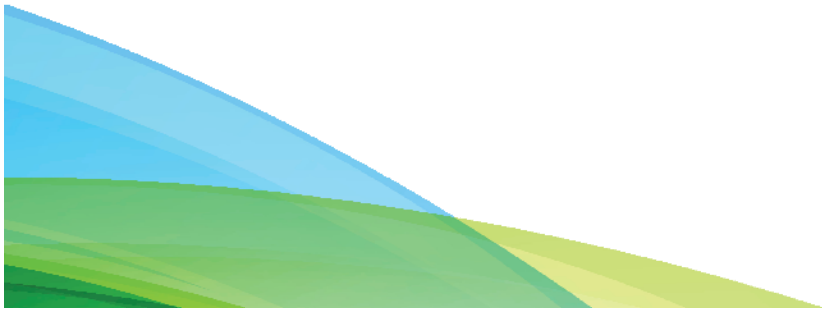
- Civil actions by injured plaintiffs are not precluded.

State Data Security Laws – New York

- On March 1, 2017, the New York Department of Financial Services ("DFS") Cybersecurity regulations ("DFS Cyber Regs") became effective. The DFS Cyber Regs impose cybersecurity requirements on those entities supervised by the DFS that are doing business in New York and "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" of New York, such as banks and insurance companies. ("Covered Entities"). [23 NYCRR Part 500 (Financial Services Law)].
- Some of the key requirements are as follows:
  - Implement and maintain an internal cybersecurity program to protect the "confidentiality, integrity and availability of the Covered Entity's Information Systems;
  - Implement written policies and procedures concerning risk assessment and conduct risk assessments of the Covered Entity's Information Systems periodically, and must implement a written incident response plan;

State Data Security Laws – New York *(cont'd)*

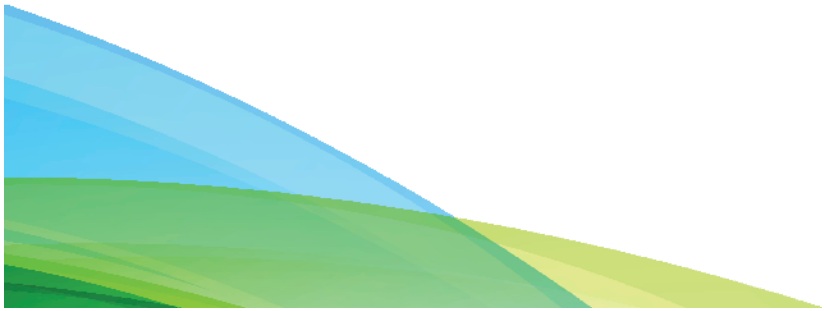
- Implement written policies and procedures concerning third-party service providers;
- Designate a qualified individual to oversee and implement the Covered Entity's cybersecurity program and enforce its cybersecurity policy, serving as Chief Information Security Officer ("CISO") or comparable position;
- Conducting of penetration testing and vulnerability assessments;
- Notification to the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred;
- Annual reporting to the DFS superintendent, certifying that the Covered Entity is in compliance with the DFS Cyber Regs;
- Annual reporting on cyber to the board of directors, a comparable governing body, or a Senior Officer if no such governing body exists;
- Limiting access privileges to Information Systems that allow access to non public information;



State Data Security Laws – New York *(cont'd)*

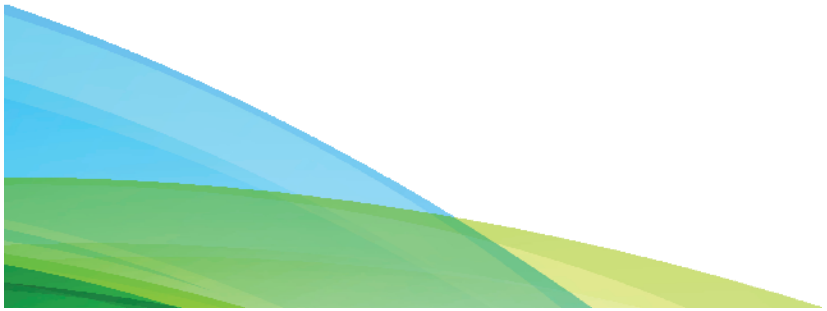
  - Encryption in transit over external networks;
  - Continuously Trained Cybersecurity Personnel;
  - Maintenance of audit trail systems.

- Some requirements must be in place within 180 days of March 1, 2017, while others have start dates of one year, 18 months, or two years.
- Limited exemptions mainly intended for small businesses.
- New York Labor Law, § 203-d ("NY Labor Law") contains a provision restricting an employer from communicating "personally identifying information" to the general public.
- "Personally identifying information" is broadly defined to include a social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number.



State Data Security Laws – New York *(cont'd)*

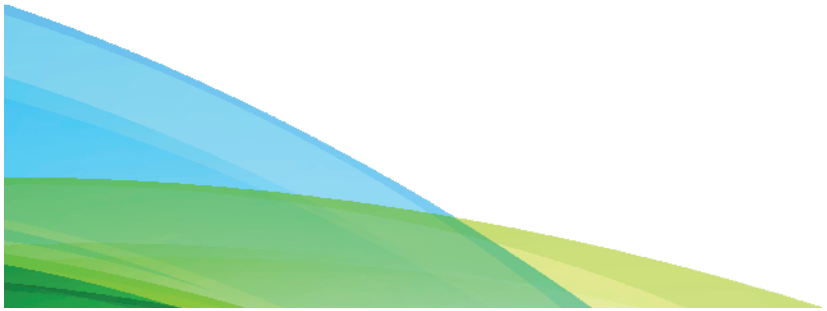
- The NY Labor Law builds in a presumption that an employer knowingly violated this section if it did not have policies and procedures in place to safeguard against personally identifying information from being disclosed to the public.
- Any knowing violation of the NY Labor Law can result in a civil penalty of up to five hundred dollars.
- It is unclear as to whether an employer and its employees must be located in New York for this law to apply or whether it be applied if only one of the parties works and/or is located in New York.
- NYC Department of Information Technology & Telecommunications has published Citywide Information Security Policies and Standards that all NYC agencies, employees, contractors, and vendors are required to follow.



European Union General Data Protection Regulation (GDPR)

Introduction to GDPR

- **Privacy Law in the EU – History**
  - Since 1995, data protection in the EU has been governed by the EU's Privacy Directive
  - Member States had to pass their own data protection laws (e.g. UK's Data Protection Act 1998)
  - In April 2016, the European Parliament passed the General Data Protection Regulation ("GDPR") which goes into effect **May 25, 2018**
- **GDPR Goals**
  - Promote uniformity of data privacy laws within the EU
  - Protect EU citizens from data breaches and provide increased control over personal data
  - Change organizational approaches to data security

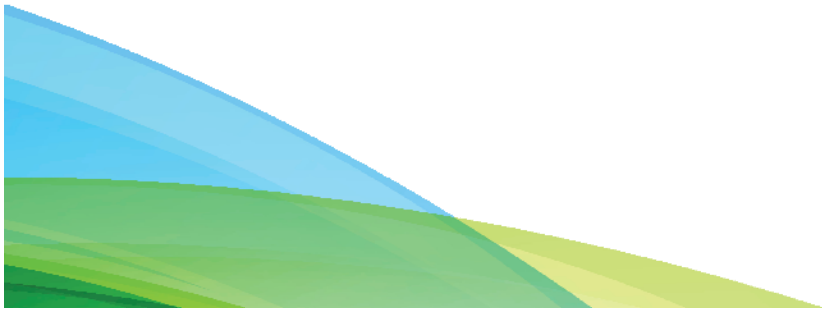


GDPR Highlights

- **New and Expanded Requirements**
  - Onerous new obligations for companies that collect or process EU citizens' personal data, regardless of location (extremely broad requirements, extraterritorial scope)
  - Confers broad rights on data subjects
- **Massive Penalties – Two Tier System**
  - *Minor violations*: Maximum fine of **€10 million or 2%** of prior year's global revenue (whichever is greater)
  - *More serious violations*: Maximum fine of **€20 million or 4%** of prior year's global revenue (whichever is greater)
  - Fines and penalties also possible under laws of particular EU Member States
- **Recent Developments**
  - Article 29 Working Party has issued several implementation guidelines
  - UK's Information Commissioner's Office published some guidance documents and others pending
  - Germany recently passed federal statute aligning German laws with GDPR

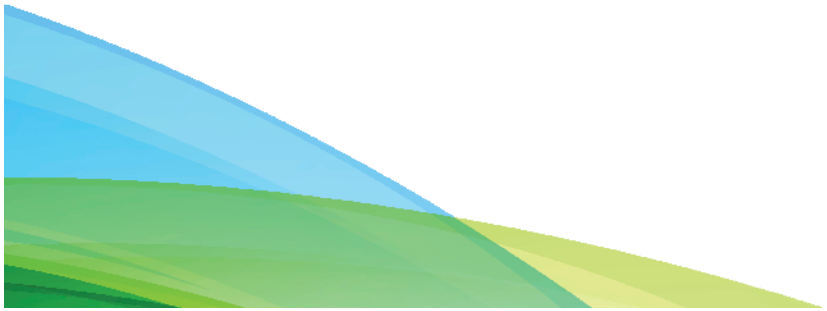
GDPR – Expanded Requirements

- **Notice:** More involved than before, language must be easily understood, concise
- **Consent:** Requires unambiguous affirmative action; must keep records to demonstrate compliance, and provide means to withdraw consent
- **Security:** Flexibility to use "appropriate" security – look at state of the art, cost, nature of data -- but greater uncertainty; required DPIA for certain controllers
- **Vendor Management:** Both controllers and processors responsible for GDPR compliance; contracts must clearly delineate responsibility
- **Cross-border Data Transfers:** New sources of model contract clauses



GDPR – New Requirements

- **DPOs:** Certain controllers must have a DPO to monitor compliance and advise business; some countries have had similar requirements, but new for EU-level law
- **DPIA:** Certain controllers will have to perform a data protection impact assessment, and the results of that assessment will determine the breadth and depth of its cybersecurity programs.
- **Data Breach Notification:** Not unfamiliar from US law, but broader notification trigger than most US laws and extremely short (72 hour) notification window place emphasis on planning ahead.



Questions

Elizabeth Gray
Partner
Washington
+1 202 303 1207
egray@willkie.com

James Burns
Partner
Washington
+1 202 303 1241
jburns@willkie.com

Norman Bay
Partner
Washington
+1 202 303 1155
nbay@willkie.com

Neal Kumar
Associate
Washington
+1 202 303 1143
nkumar@willkie.com

Katherine Hanniford
Associate
Washington
+1 202 303 1157
khanniford@willkie.com