

**Identifying Challenges and  
Developing Effective WSPs for  
Outsourcing to Third-Party  
Vendors**

**Financial Markets Association  
Securities Compliance Seminar  
April 24, 2025**





# Introduction of Our Panel Members

- Loren Lopez, CP, FRP, Senior Director, Vendor Management & Senior Paralegal, TradeStation Securities, Inc.
- Keith Bettencourt, Director, Cybersecurity Group, FINRA
- Marc B. Minor, Senior Counsel, Thompson Hine, LLP
- Bill Reilly, Director, Oyster Consulting, LLC



# What Do We Hope to Accomplish Today

- Discuss the Rules and Regulations Governing and Regulators Expectations of Compliance
- Discuss a Framework for Effective WSPs and Implementation
- Selection, Monitoring and Meeting Performance Measures
- Technology/Security Issues
- Assigning Risk
- Other Third-Party Vendor Challenges



# Regulatory Rules, Programs and Expectations

- Reg. S-P Rule Updates
  - Vendor Management
    - “require oversight of ‘service providers’ to ensure they
      - protect against unauthorized access to or use of customer information; and
      - provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware of a breach
  - Incident Response – detect, respond, and recover
    - Customer notification requirements
  - Compliance dates of Dec. 3, 2025 (larger entities) or June 3, 2026 (smaller)
- FINRA Vendor Questionnaire 2.0
- Cybersecurity Advisory – NIST Releases Version 2.0 of its Cybersecurity Framework



# Firm WSPs, Controls, Technology and Challenges

- Regulatory Notice 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
- Importance of effective WSPs for outsourcing to third-party vendors
- Effective VRM processes and procedures include the continuous life cycle for Vendor relationships:
  - Planning
  - Due diligence and vendor selection
  - Contract facilitation and negotiation
  - Ongoing monitoring and supervision
  - Termination



# Firm WSPs, Controls, Technology and Challenges

- VRM Stakeholder Reviews (OFAC/AML, Compliance, Information Security, Privacy (as applicable), Legal and Risk)
- Emerging Risk: Artificial Intelligence – Assess whether the vendor's services include the use of AI
- Vendor Risk Classification
- Governance



# Legal and Consulting Issues

- Common Observations and Issues
  - WSPs/Controls
  - Business continuity procedures
  - Risk
  - Technology
  - Review /Observations
  - Matters Requiring Attention/Best Practices



# Legal and Consulting Issues

- Business continuity procedures
- Material data breach reporting obligations (public cos.)
  - SEC Release Nos. 33-11216, 34-97989 (eff. 9/5/23) (Materiality definition) TSC Industries, Inc. v. Northway, Inc., Basic, Inc. v. Levinson, and Matrixx Initiatives, Inc. v. Siracusano
  - “the definition of ‘information systems’ contemplates those resources owned by third parties and used by the registrant. . .” (33-11216)
- SolarWinds Orion incident.
- Flagstar Financial, Inc./ Citrix Breach.  
(<https://www.sec.gov/files/litigation/admin/2024/33-11343.pdf>).
- State Issues. See NY Cyberreg NY CRR 500