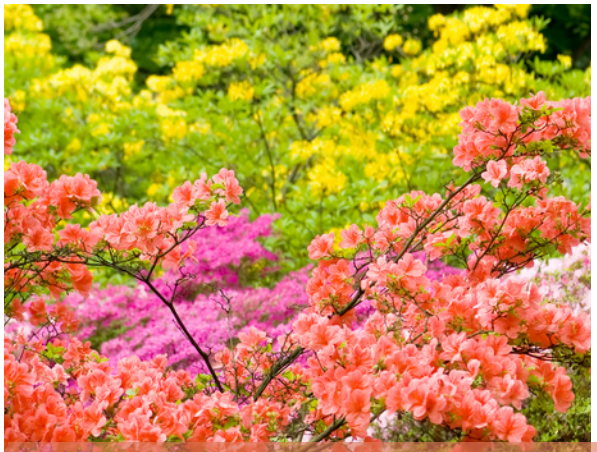
EXCHANGE ANALYTICS
Regulatory Compliance Solutions

April 2023

QUARTERLY CLIENT NEWSLETTER



Happy spring, everyone! *Conference season* is upon us again, and we look forward to catching up with some of you in person. We will be attending the following conferences over the next few months:

- **NASAA Public Policy Symposium, DC | April**
- **FIA Law &Compliance, DC | April**
- **ARM Educational, FL | June**

Please reach out to us if you will be at any of these conferences. We would like to connect with you and be available to answer any compliance training questions.

IS IT TIME TO MAKE THE SWITCH TO *MONTHLY INVOICES?*

Monthly or quarterly invoices reduce administrative burden and provide a more streamlined and efficient billing process.

Contact **info@xanalytics.com** for more information.

FAQ CORNER

Our most frequently asked questions from clients.

- Do you have a **Course Catalog**?
  - Yes! Access HERE.
- Is there a **Branch Admin Guide**?
  - Our updated Branch Admin Guide is now available!
- How do I access **Course Outlines**?
  - Access our latest outlines on our website under RESOURCES.

Can't find what you're looking for? Find our complete FAQ compilation on our website.

NEW COURSES COMING SOON!

FOREIGN CORRUPT PRACTICES ACT (FCPA) |

Combat bribery and corruption in international business transactions. Ensure your employees are trained in promoting fairness in international business, fighting corruption, protecting national security and upholding corporate responsibility.

FINANCIAL EXPLOITATION OF SPECIAL ADULTS |

Financial exploitation of special adults is a serious crime, and laws have been enacted to protect vulnerable adults from this type of abuse. Financial exploitation can take many forms, including theft, fraud, forgery, embezzlement, identity theft, and undue influence.

ION MARKETS: THE FUTURE OF RISK MANAGEMENT?

BY MEGAN CONLEY | HEAD OF OPERATIONS, XA

The ION Markets ransomware attack in January has raised a number of questions about the interconnectedness of firms and the risk third-party vendors pose to the systemic health of the derivatives industry.

Firms should examine proactive and reactive capabilities.

The attack by LockBit, the world's largest and most active ransomware gang, triggered trade reporting delays and industry reliance on manual processes. Despite delays, the event demonstrated the professionalism and resiliency of the industry; however, vulnerabilities in shared service providers highlighted potential weaker links in industry infrastructure.

Outsourcing non-core business functions is a common practice. Third-party service providers are essential for business operations; however, with the benefit comes potential operational, legal, financial and reputational risk.

Firms should examine what proactive measures (due diligence, risk policies, vendor contract language, employee training) and reactive capabilities (incident response planning, coordination of risk management protocols) they currently have in place.

How should third-party service provider risk be managed?

In 2021, the National Futures Association adopted Interpretive Notice 9079 – NFA Compliance Rules 2-9 and 2-36: Members' Use of Third-Party Service Providers requiring Members to adopt a written supervisory framework overseeing outsourced regulatory functions by third-party service providers.

In 2022, the European Council adopted the Digital Operational Resilience Act ("DORA") with technical standards anticipated to be released this year with an implementation deadline of January 17, 2025. DORA will require EU financial service entities to adopt risk management policies related to ICT incidents and also provides oversight authority of third-party service providers used by those entities.

The CFTC continues to discuss and explore the need for additional guidance around the use of third-party vendors.

The response by regulators raises questions about what jurisdiction, if any, they have to monitor service providers. Do they have the resources to do so effectively? Also, what responsibility and resources do firms have to effectively police service providers they use? How can they assess and enforce the practices of providers? Beyond jurisdictional and resource questions, how should third-party service providers be categorized? Do the vendors have direct access to your system? How are they connected? What services do they provide and how much risk do they pose? No one vendor is alike so how can we categorize their risk level?

There is no clear answer to any of these questions, and as we all know, it is not a matter of "if" but "when" a cyber-attack will occur. The ION event is an opportunity for the industry to engage in discussion and identify practical ways to further safeguard against cyber-attacks and create a more secure and resilient marketplace.