EXPERT NETWORK UPDATE

Top Risk Management & Compliance Controls H1/2025

Headline: *Risk and Compliance headwinds for Expert Networks and their clients in H1 are due to: (1) increased competition, margin compression, AI and tech-driven products & services; (2) an anticipated decrease in regulatory supervision and enforcement; and (3) ongoing geopolitical, cross border and cyber threats.*

An increase in data loss and fraud is likely, with private litigation expected over the longer term to fill the supervisory void. A material regulatory event and return to enforcement should not be discounted given well-reported "animal spirits," particularly if they run unchecked.

Action: *Market participants should adapt and leverage well-defined Risk Management & Compliance disciplines as they move through 2025. The end result: an ability to move fast, deliver results, protect crown jewels and avoid own goals.*

TOP RISK MANAGEMENT & COMPLIANCE CONTROLS

Model Risk Management
- Artificial Intelligence
- Vendor Risk
- Concentration Risk
- Internal IP Leakage
- External IP Theft

Enhanced Due Diligence
- Expert Fraud
- ID Theft & Deepfakes
- Sanctions / OFAC Violation
- Project Risk
- MNPI

Legal Risk Management
- Target Company Lawsuits
- Class Actions
- Spamming
- Insider Trading

Conduct Risk Management
- Margin Compression
- Culture of Compliance
- Employee Capture
- Off Channel Communications
- Diversity & Merit
- Employee Satisfaction
- Talent Flight

Cybersecurity
- Cyber Insurance
- Pen Test
- Data Breach Resilience

Geopolitical & Cross Border Risk Management
- China: Sensitive Data, High Risk Industries
- India
- Middle East
- Bribery, Corruption
- Regulatory Change Management

I. MODEL RISK MANAGEMENT

The headline is, of course, Artificial Intelligence (AI) – risks *and* opportunities. Market participants are taking a measure of comfort that best practices exist when it comes to Model Risk Management, including controls around Vendors and even Concentration Risk, i.e., not relying heavily on any one provider. However, service providers are also *improving* internal guidance and monitoring employee behaviors to protect IP and Confidential Information from public disclosure by even the most well-intentioned employees using tools like ChatGPT, Claude and Gemini.

Externally, IP – in the form of New Products & Services – and Information Security are both at increased risk, particularly in the Middle East, APAC and China, as third parties and especially local participants exploit various methods, including AI, to violate user terms and conditions, exfiltrate data and reverse engineer proprietary products.

II. ENHANCED DUE DILIGENCE

One control that deserves serious emphasis is Enhanced Due Diligence (EDD) given its ability to combat Expert Fraud and ID Theft, including the rise of Deepfakes. At onboarding and during the expert relationship, well-functioning EDD offers material compliance ROI with global Sanctions and OFAC requirements and, more broadly, Project Risk, i.e., its true purpose and end-beneficiary, protecting MNPI and preventing Insider Trading. While that might not be a high risk for top performing firms, service providers must manage a variety of client types, risk tolerances and geographic realities.

III. LEGAL RISK MANAGEMENT

We are hearing about excitement and enlivened "animal spirits" across markets. Companies will move faster in their industries, and so a long time motto deserves a slight adjustment: Move fast, *yes.* Just don't break the *wrong* things.

In this light, the threat of Litigation for providers over the medium and longer terms deserves a renewed review and strengthening. Plaintiffs' actions on behalf of Target Companies and Class Actions could likely fill the void created by federal regulators lightening their supervision and decreasing their enforcement actions. Spamming experts, experts violating Non-Disclosure & Confidentiality Agreements, and other Employee Conduct issues noted below, particularly in foreign jurisdictions, are worth including or increasing in monitoring and testing programs.

Given Expert Networks' role in Technology and Financial Services, as well as other regulated sectors, e.g., Health Care and Defense, service providers should proactively review or develop a risk-based strategy and their Litigation Defense Playbooks that align with these new market dynamics. Checks in with providers occur, but this quarter is a good time to ensure everyone remains on the same page. Longer term, the return of regulatory scrutiny is inevitable, but should anything material "break" and draw public scrutiny sooner, the lifecycle of free market begets crisis begets regulation begets enforcement will move on from the present day's state.

Positively, and even acknowledging animal spirits (the phrase of January 2025), mature market participants, clients and service providers alike, aren't seen to have any appetite to contribute to any undue Insider Trading risk. Nonetheless, new and emerging participants, take note.

IV. EMPLOYEE CONDUCT RISK MANAGEMENT

The industry's growth is also directly impacting Conduct Risk. New market participants and Margin Compression are threats to the industry's Compliance Standards and rules of engagement with clients, service providers, experts and even competitors. To these ends, promoting the importance of defending against Employee Capture and Off Channel Communications, particularly in emerging markets and jurisdictions with lax enforcement, are critically important. Whether by an expert or even the best of any user firm's rogue employee or an employee of the service provider itself, MNPI is enticing and can be incentive to violate policies, particularly in APAC and the Middle East.

One previously material issue deserves discussion at its parts. ESG had been garnering attention and significant resources over the past four years. It has fallen off everyone's list, with a few caveats. Diversity and Merit directly impacts Employee Satisfaction, Talent Flight and, particularly in the EU, Investments and Acquisitions. Overcorrections should be guarded against, as employees may interpret them a departure from core principles of equity and advancement. These could eat at a firm's overall Culture, including Compliance, if not guarded against.

This is not an original statement: Market participants should consider how to manage certain underlying issues that matter without focusing on how they are collectively labeled or packaged.

V. CYBERSECURITY

For some pre-existing high risks, we suggest nuanced attention. Firms should ensure the full scope of their Cyber Insurance is understood, for example, and does not leave any material gaps. The cautionary tale unfolding in California, where residents and businesses are discovering policy changes, coverage gaps and rising premiums.

Annual Pen Tests and Incident Response exercises are worth management's time and effort, the former providing technical comfort, the latter resilience when it comes to well-performing human behaviors. Market participants *could* scope these further to ensure controls are operating as intended when it comes to PII, the largest client names and most sensitive projects.

VI. GEOPOLITICAL & CROSS BORDER RISK MANAGEMENT

Geopolitical Risk between the U.S. and China remains, particularly regarding Sensitive Industries such as semiconductors, AI, quantum computing, EV, military and defense technology. As noted, market participants in and around Mainland China should view EDD as critical in controlling against the unintentional engagement of experts affiliated with State Owned Enterprises (SOEs) and the direct implication of Bribery or Official Corruption, particularly should tensions rapidly escalate.

More broadly, in addition to new Products & Services, decreased supervision and enforcement and the above animal spirits, market participants are entering new jurisdictions requiring Cross Border legal, risk and compliance know how and capabilities to address expanding Global Regulatory Changes.

CONCLUSION

Firms should embrace the moment while executives risk-scope their Governance, Risk and Compliance Programs. Leverage pre-existing controls. Expand and adapt. Be communicative – with employees and clients alike of all intentions to meet these new animal spirits head on. Consider the next Due Diligence or Surveillance Calls as an opportunity to flex and give comfort.

Contact:
Paul Caulfield
PCAULFIELD@RUDDYLAW.COM
+1-212-495-9506

Paul Caulfield heads the firm's Financial Regulation and Cybersecurity Practices. Before entering private practice, Paul held global positions in financial services across legal, risk, compliance and operations. Paul is certified in Information Systems Security (CISSP) and Anti-Money Laundering (CAMS), holds his Series 24, 7 and 66 licenses and is an Adjunct Professor at Fordham University School of Law. He began his career with the Manhattan District Attorney's Office.

INVENTORY OF LEGAL & GRC RISKS

~ EXPERT NETWORKS ~
as of January 2025

A
Anti-Money Laundering
Antitrust
Artificial Intelligence
APAC

B
Board of Directors
Bribery
Budget Management
Bullying, Online
Bullying, Workplace
Business Continuity

C
China
Class Action
Commissions
Compliance Risk Management
Concentration Risk, Client
Concentration Risk, Vendor
Conduct Risk
Confidential Information
Conflicts of Interest
Consumer Protection
Contracts
Corporate Espionage
Corporates
Corruption
Country Risk
Credit, Private
Crisis Management
Cross Border Data Transfers
Cybersecurity

D
Data Protection
Dawn Raid
Deepfakes
Disaster Recovery
Diversity
Dubai

E
Employee Capture
Employee Conduct
Employee Satisfaction
Enhanced Due Diligence – Client, ESG
Equities
Ethics
Expert, Project

F
Financial Conduct Authority (UK)
Fraud, Client, Employee, Expert, Vendor

G
Geopolitical Risk Management
GDPR – General Data Protection Regulation
Governance
Government Action, Investigations

H
Harassment, Online
Harassment, Workplace
Hedge Funds
Hong Kong Monetary Authority
Hong Kong SAR

I
Identity Theft
Incentive Compensation
Incident Response
India
Information Security
Insider Trading
Insurance, Cyber
Intellectual Property
Investment Bank
Investor Protection

J
Japan
Joint Venture

K
Know Your Customer

L
Litigation, Defense
Litigation, Plaintiff

M
Management Consulting
Mandatory Reporting
Margin Compression
Market Abuse
Material Non-Public Information (MNPI)
Mergers & Acquisitions
Middle East
Misappropriation
Model Risk Management, AI, LLM

N
Non-Compete Agreement
Non-Disclosure Agreement

O
OFAC
Off Channel Communications
Operations Risk Management
Outside Business Interests

P
Penetration (Pen) Test
Personal Identifying Information (PII)
Politically Exposed Persons
Privacy
Products and Services
Project Risk
Private Equity

R
Regulatory Change Management
Reputation Risk Management
Russia

S
Sanctions
Saudi Arabia
Securities and Exchange Commission (US)
Security, Online
Security, Physical
Sensitive Industries, Sectors & Topics
Singapore
Spam
South Korea
State Owned Entity (SOE)
Succession Planning
Surprise Inspections, also Dawn Raids

T
Talent Risk Management
Target Companies
Tax Compliance
Theft, External
Theft, Internal
Third Party Risk Management

U
Ukraine
Unfair Business Practices
United Arab Emirates

V
Vendor Risk Management
Vietnam

W
Wage and Hour Compliance
Whistleblower
Workplace Safety, including Remote