Thank you for joining today's FIA Law and Compliance Division webinar.

We will begin momentarily.

Cleared for Risk

Cyber, Privacy & AI Threats Facing the Derivatives Industry

Cyber threats are no longer just an IT problem — they're a clearing risk, a regulatory risk, and a boardroom risk.

Presented at the Futures Industry Association (FIA)

Aaron Charfoos
Partner & Co-Chair, Data Privacy and Cybersecurity | Paul Hastings LLP

Michelle A. Reed
Partner & Co-Chair, Data Privacy and Cybersecurity | Paul Hastings LLP

Reminders:

- This webinar will be recorded and posted to the FIA website within 48 hours of the live webinar.
- Please use the “question” function on your webinar control panel to ask a question to the moderator or speakers.
- Disclaimer: This webinar is intended for informational purposes only and is not intended to provide investment, tax, business, legal or professional advice. Neither FIA nor its members endorse, approve, recommend, or certify any information, opinion, product, or service referenced in this webinar. FIA makes no representations, warranties, or guarantees as to the webinar’s content.

Session Overview

ION Markets Attack & Lessons

Case study: when a single vendor takes down an industry

Evolving Threat Landscape

AI-enabled adversaries targeting derivatives markets

Systemic Risk & 24/7 Trading

Why cyber is a clearing problem

CFTC, NFA & SEC Cyber Rules

Your primary regulators on cybersecurity

DOJ Bulk Data & Global Privacy

Cross-border data rules for derivatives firms

AI Framework & Vendor Risk

Governance for trading ecosystems

Incident Response & Board Governance

The Three R's for cleared markets

FIA Taskforce & Key Takeaways

Your industry playbook for resilience

All content framed for clearing firms, exchanges, FCMs, clearinghouses, and market infrastructure providers.

Aaron Charfoos

Partner
Paul Hastings LLP
Chicago

aaroncharfoos@paulhastings.com
+1.312.499.6016

Co-Chair, Data Privacy and Cybersecurity Practice

Chair, Chicago Litigation Department

- Chambers-ranked cybersecurity, privacy, class action, and data protection trial lawyer
- Litigated data breach class actions, VPPA, BIPA, CIPA, and pixel/tracking technology cases
- Advises on the intersection of AI, data privacy, and cybersecurity, including data governance and algorithmic bias
- Guided clients through data breaches affecting tens of millions of individuals
- Defends clients in regulatory investigations by U.S. federal regulators, state AGs, and international bodies

Michelle A. Reed

Partner
Paul Hastings LLP
Dallas

michellereed@paulhastings.com
+1.972.936.7475

Co-Chair, Data Privacy and Cybersecurity Practice

CIPP/US (IAPP) | Chambers Global & Chambers USA Ranked

- Two decades advising companies, boards, and executives on privacy and cybersecurity regulation, enforcement, and litigation
- Crisis management leader: data breach response, SEC cybersecurity compliance, regulatory investigations, AI/biometrics/children's privacy
- *Chambers describes her as "incredibly responsive and super knowledgeable"*
- Represents clients in securities class actions, derivative suits, and consumer class actions
- Awards: Legal 500 Cyber Law, Lawdragon 500, Cybersecurity Docket Incident Response, Texas Trailblazer

When a Single Vendor Goes Down

The ION Markets Ransomware Attack — January 31, 2023

700+

Individuals joined FIA's crisis calls within one week

2 wks

Recovery time for some impacted clearing firms

3+ wks

CFTC Commitment of Traders report delayed

- LockBit ransomware hit ION Markets, a third-party provider of middle- and back-office products embedded in clearing workflows at dozens of firms globally
- Trade processing disrupted across Europe, Asia-Pacific, and the Americas; firms manually reconstructed trading records
- FIA held 4 conference calls on day one alone; notified CFTC, Bank of England, BaFin, AMF, Finansinspektionen
- Key lesson: the entire exchange-traded and cleared derivatives ecosystem is only as strong as its most critical third-party service provider
- Led directly to FIA's Cyber Risk Taskforce and six recommendations for strengthening industry resilience

Source: FIA Taskforce on Cyber Risk — After Action Report and Findings, September 2023

The Evolving Threat Landscape for Derivatives Markets

89%

YoY increase in AI-enabled adversary operations

29 min

Average eCrime breakout time (fastest: 27 sec)

82%

Of 2025 detections were malware-free

- Financial services is the 4th most-targeted sector (12% of all activity); 43% spike in hands-on-keyboard intrusions against financial institutions
- Access broker activity surged 50% YoY; 423 financial firms appeared on dedicated leak sites (+27% YoY)
- For FCMs and clearing firms: a breach that compromises trade processing, margin calculations, or customer segregated funds is not just a data breach — it's a market integrity event
- Attackers log in with valid credentials, they don't hack in — identity-based intrusions dominate: 5 of top 10 MITRE ATT&CK tactics are identity-based

Sources: CrowdStrike 2026 Global Threat Report; CrowdStrike 2026 Financial Services Report

Systemic Risk: Why Cyber Is a Clearing Problem

Interconnected Ecosystem

- Exchanges → CCPs → clearing members → end clients all depend on shared infrastructure
- A ransomware attack on a single vendor (as ION showed) can disrupt settlement, margin calls, position management, and regulatory reporting across jurisdictions
- FIA created an Industry Resilience Committee (IRC) of clearing firms, vendors, exchanges, and CCPs to address systemic risks

Emerging Threat Vectors

$2.02B

in digital assets stolen in 2025 by North Korean actors (51% YoY increase)

- FAMOUS CHOLLIMA doubled operations using AI-generated identities to infiltrate crypto exchanges and fintech
- 35% of cloud incidents from valid account abuse
- AI infrastructure as attack surface: 90+ orgs exploited via prompt injection

Sources: FIA Taskforce Report 2023; CrowdStrike 2026 Global Threat Report

CFTC & NFA: Cyber Requirements for Derivatives Firms

Your Primary Regulators on Cyber

CFTC Rule 160.30

System safeguards for intermediaries — applies to FCMs, swap dealers, major swap participants. Requires information security protections for customer data.

Proposed ORF (Dec 2023)

Would require FCMs, SDs, and MSPs to establish an Operational Resilience Framework covering: (1) IT security, (2) third-party relationships, (3) emergencies and disruptions.

CFTC Parts 38 & 39

System safeguards for DCMs (exchanges) and DCOs (clearinghouses): cybersecurity testing, vulnerability assessment, incident response.

NFA Requirements

Written information security program; risk assessment; incident response plan; employee training; vendor oversight. Applies to all NFA member firms.

These are the rules that directly govern FIA members as FCMs, exchanges, and clearinghouses

Sources: CFTC proposed rule Dec 2023; FIA MarketVoice; NFA compliance standards

SEC Cyber-Incident Disclosure: When It Applies to You

Not all FIA members are SEC registrants — but many are: publicly traded exchanges (CME, ICE, Cboe), clearing firms that are also registered broker-dealers, and public holding companies

60%

Increase in disclosed cyber incidents

78%

Disclosures within 8 days of discovery

1 in 4

Breaches from third-party vendors

- Item 1.05 Form 8-K: material incidents disclosed within 4 business days of materiality determination
- Item 106 Reg S-K: annual disclosure of cybersecurity risk management, governance, and board oversight
- Threat actors used SEC rules as extortion tactic — filing whistleblower reports about victims' failure to disclose
- Even non-public FIA members should track these rules: your public counterparties' disclosure obligations affect you

Source: Paul Hastings SEC Cybersecurity Incident Disclosure Report, December 2024

DOJ Bulk Data Transfer Rules: Cross-Border Impact

EO 14117: Preventing foreign adversary access to Americans' bulk sensitive personal data | Final Rule effective April 8, 2025

Countries of Concern

China (incl. HK, Macau) | Cuba | Iran
North Korea | Russia | Venezuela

Why This Matters for Derivatives Firms

- FCMs and clearing firms handle massive volumes of customer financial data
- Firms with offshore processing, foreign affiliates in countries of concern, or cross-border vendor relationships must assess covered transactions
- Exception certain financial services transactions 28 CFR 202.505

Transaction Types

Prohibited: data brokerage with countries of concern; bulk human 'omic data

Restricted: vendor, employment, and investment agreements (permitted only if CISA security requirements met)

Covered data: personal identifiers, financial data, geolocation, health data, biometric identifiers

Sources: DOJ Final Rule 28 CFR Part 202; Paul Hastings Client Alert Feb 13, 2025

DOJ Bulk Data: Compliance for Derivatives Firms

Apr 8, 2025

Most provisions effective

Jul 8, 2025

90-day leniency period expired

Oct 6, 2025

Audit, due diligence, recordkeeping

Penalties: Civil fines up to $368,136/violation or 2x transaction value | Criminal: up to $1M and/or 20 years

- Annual audit and officer certification required for restricted transactions
- Practical challenges for FCMs: mapping data flows across prime brokerage, clearing, and settlement; determining whether aggregate 12-month transfers meet bulk thresholds
- Must contractually prohibit onward transfer of data to countries of concern with all foreign vendor counterparties
- Full and accurate records of all covered data transactions required

Sources: DOJ NSD Compliance Guide Apr 2025; Paul Hastings Client Alert Apr 17, 2025

State & International Data Privacy: The Patchwork Problem

20+

U.S. states with comprehensive consumer privacy laws

- FIA members collecting customer data across multiple states face a compliance matrix: different notice, consent, and opt-out requirements
- Many state laws include automated decision-making and profiling provisions — affecting algorithmic trading and risk tools

GDPR

Fines up to €20M or 4% revenue; strong enforcement of AI uses; applies to FIA members with EU operations or clients

EU DORA

Effective Jan 2025. Multi-stage incident reporting: initial notification within 4 hours of classifying as major (or 24 hours from detection); intermediate report within 72 hours; final report within 1 month. Impacts EU exchanges, CCPs, clearing firms, and critical ICT service providers.

Regulation S-P

Safeguarding nonpublic personal information — applies to broker-dealers and investment advisers (incl. dually-registered FCMs)

FIA has urged the European Commission to clarify that financial services are not "ICT services" under DORA

Sources: FIA DORA statement Jan 2025; GDPR; EU AI Act; DORA Regulation 2022/2554, Article 19; Regulation S-P

AI-Driven Decision-Making: Regulatory Framework for Derivatives

CFTC Position

FIA urged “technology-neutral” approach (joined by CME, ICE, FIA PTG); existing rules provide needed controls; new AI-specific rules may not be necessary

SEC Exams (FY 2026)

Focused on AI technologies, automated tools, trading algorithms — affects dually-registered FCMs and public exchange operators

FINRA (Dual Registrants)

2026 Annual Oversight Report: GenAI section; AI agents as emerging trend (Jan 2026); risks: autonomy, auditability, data sensitivity

AI in Derivatives Today

Algorithmic trading, risk modeling, margin optimization, surveillance, AML detection, client onboarding — all subject to existing supervisory requirements

Key principle: AI deployed in clearing or trading systems must meet existing supervisory, risk management, and system safeguard requirements — there is no “AI exception”

Sources: FIA comment letter to CFTC; FINRA 2026 Oversight Report; SEC FY 2026 exam priorities

Third-Party Vendor Risk in Trading Ecosystems

The ION attack proved that third-party risk is THE defining cybersecurity challenge for cleared derivatives markets

- Many participants rely on third parties for mission-critical services: market data, trade processing, reconciliation, collateral management, risk calculations
- FIA Taskforce Recommendation #5: standardize third-party risk assessment questionnaires; calibrate risk management to type of service and impact of disruption
- CFTC Proposed ORF: explicitly covers “third-party relationships” as one of three core risk areas
- EU DORA: establishes oversight framework for critical third-party technology service providers — may designate major trade processing vendors as “critical”
- DOJ Bulk Data Rule adds another layer: vendor agreements with foreign persons must contractually prohibit onward data transfer to countries of concern
- Exchange connectivity: member firms have independent notification obligations to exchanges when cyber incidents impact trading or communications — distinct from regulatory reporting

> *“Before you sign up with a third party, conduct your due diligence — that includes financial stability, but also diligence around cyber controls, business continuity and data resilience.” — Tom Wagner, SIFMA (FIA Boca 2023)*

Sources: FIA Taskforce Report 2023; CFTC proposed ORF; FIA Boca panel

Incident Response for Cleared Derivatives Markets

29 min
Average breakout time
Response in minutes, not hours

4 days
SEC 8-K disclosure window
for public company members

Three R's
FIA's framework:
Response, Recovery, Reconnection

- Response: coping with immediate impact; CFTC/NFA require prompt notification of material cybersecurity events
- FinCEN SAR: a cyber event that facilitates or is intended to facilitate a suspicious transaction requires a Suspicious Activity Report within 30 days — FCMs have BSA/AML filing obligations that can be triggered by cyber incidents
- Exchange notifications: exchange rules independently require member firms to notify when a cyber incident impacts the firm's ability to trade or communicate with the exchange — these obligations run parallel to and are separate from regulatory reporting
- Recovery: rebuilding systems and databases; ION recovery took up to 2 weeks with manual reconstruction
- Reconnection (the hardest part): reconnecting to exchanges, CCPs, service providers; disparate attestation requirements added delay during ION incident
- Unique considerations: settlement finality, margin obligations, customer segregated funds, position management, counterparty exposure
- FIA recommends adoption of FSSCC (US) and CMORG (UK) reconnection guidelines for the derivatives industry
- *Emerging: CISA is expected to issue final guidance this month on critical infrastructure cyber incident reporting under CIRCIA — financial services firms, including clearing firms and exchanges, may be covered entities; firms should monitor for the final rule and assess applicability*

Sources: FIA Taskforce Report 2023; Paul Hastings SEC Disclosure Report 2024; 31 CFR 1026.320; CISA CIRCIA rulemaking (final rule expected Sept 2026)

Board-Level Governance of Cyber and AI Risk

- SEC rules: annual disclosure of board's cybersecurity oversight (for public companies)
- Delaware law: Caremark duty to monitor extends to cybersecurity oversight

Key Questions for Boards at Clearing Firms, Exchanges, and FCMs

1 Do we have visibility into AI use across trading, clearing, and compliance?

2 Is cyber investment keeping pace with the 89% YoY increase in AI-enabled attacks?

3 Have we stress-tested for a critical vendor going down (ION scenario)?

4 Do board materials include cybersecurity metrics specific to our market infrastructure role?

5 Are we prepared for overlapping obligations: CFTC safeguards, SEC disclosure, NFA, DORA?

6 What steps secure our own and third-party AI tools from prompt injection?

For FIA members: a cyber event at a clearing firm is not just a company problem — it's a market problem

24/7 Trading: Operational Resilience Challenge

Emerging Issue for FIA Members

> *FIA (May 2025): "FIA does not support extending trading and clearing in CFTC-regulated derivatives markets to a 24/7 basis until [operational, infrastructure, risk, compliance and regulatory issues] have been systematically identified, assessed, and resolved."*

No Maintenance Windows

Today's cybersecurity relies on scheduled windows for patching and updates — 24/7 eliminates these

Continuous SOC Coverage

24/7 cyber monitoring requires staffing across all time zones

Zero Downtime Recovery

During 24/7 markets, there is no downtime to recover from a cyber incident without market impact

Framework Requirements

Strong cybersecurity frameworks including anomaly detection and zero-trust architectures would be required

Sources: FIA 24/7 comment letter May 2025; FIA 24/7 white paper

Regulatory Landscape: Summary Matrix

Regulatory Area	Key Rule/Framework	Applies To	Key Requirement
CFTC System Safeguards	Rule 160.30 Parts 38, 39	FCMs, SDs, DCMs, DCOs	Info security, BCP, testing
CFTC Proposed ORF	Proposed Dec 2023	FCMs, SDs, MSPs	IT security + third-party + disruption
NFA Cyber	NFA Interpretive Notices	All NFA members	Written ISSP, assessment, training
SEC Cyber Disclosure	Item 1.05 / Item 106	Public company registrants	4-day disclosure; annual governance
DOJ Bulk Data	EO 14117 / 28 CFR 202	All U.S. persons	Prohibit/restrict transfers
EU DORA	Regulation 2022/2554	EU financial entities & critical ICT providers	4-hr/24-hr initial, 72-hr intermediate, 1-month final report
FinCEN SAR	BSA / 31 CFR 1026.320	FCMs, broker-dealers	30-day SAR when cyber facilitates suspicious activity
State Privacy	20+ state laws	Entities collecting consumer data	Consumer rights, automated decisions
CFTC on AI	Technology-neutral approach	FCMs, exchanges	Existing rules; outcomes focus
CISA CIRCIA	Pending final guidance (Sept 2026)	Critical infrastructure (potentially incl. financial services)	72-hr incident / 24-hr ransom payment (awaiting final guidance)

FIA Taskforce Recommendations

Your Industry Playbook for Resilience

1 **Form Industry Resilience Committee**

Now operational — for crisis coordination and BAU resilience planning

2 **Connect with sector-wide groups**

FS-ISAC, FSSCC, CMORG, SIFMA for threat intelligence sharing

3 **Review reconnection policies**

Adopt FSSCC (US) and CMORG (UK) reconnection guidelines

4 **Establish ex-ante info sharing**

Pre-agreed procedures with exchanges, CCPs, and service providers for cyber incidents

5 **Standardize vendor risk assessment**

Standardize questionnaires; calibrate to service type and disruption impact

6 **Participate in cyber exercises**

Hamilton (US Treasury), Quantum Dawn (SIFMA) — incorporate derivatives scenarios

FIA Annual Disaster Recovery Exercise: 2025 test successfully completed Oct 25, 2025 | 2026 test scheduled Oct 24, 2026

Source: FIA Taskforce on Cyber Risk — After Action Report and Findings, September 2023

Key Takeaways & Actionable Strategies

1 Learn from ION

Map critical third-party dependencies; stress-test vendor outage plans

2 Map data for DOJ compliance

Identify covered transactions, cross-border flows, vendor relationships

3 Update incident response

Calibrate for 29-min breakout; practice CFTC notification and SEC 8-K

4 Implement AI governance

Inventory AI in trading/clearing/compliance; meet CFTC/NFA requirements

5 Prepare for CFTC ORF

Build framework: IT security, third-party relationships, disruption mgmt

6 Strengthen vendor contracts

Add cyber incident provisions, reconnection protocols, DOJ protections

7 Engage the board

Align governance with CFTC/SEC/NFA/DORA; include systemic risk

8 Join industry resilience

Engage FIA IRC, FS-ISAC; participate in disaster recovery exercises

9 Navigate the patchwork

Map state privacy, GDPR, DORA for EU operations

Further Reading & Resources

- FIA Taskforce on Cyber Risk — After Action Report and Findings (September 2023)
- CrowdStrike 2026 Global Threat Report
- Paul Hastings SEC Cybersecurity Incident Disclosure Report (December 2024)
- DOJ Data Security Program Compliance Guide (April 11, 2025)
- CFTC Proposed Operational Resilience Framework (December 2023)
- FIA Comment Letter on 24/7 Trading and Clearing (May 2025)
- EU Digital Operational Resilience Act (DORA) — Regulation 2022/2554
- SEC Final Rules on Cybersecurity Disclosure (July 2023)
- Paul Hastings Client Alert: DOJ Bulk Data Rules (February 13, 2025)
- CISA CIRCIA — Cyber Incident Reporting for Critical Infrastructure Act (final guidance expected September 2026)

Questions?

Aaron Charfoos

Partner | Co-Chair, Data Privacy and Cybersecurity
Paul Hastings LLP | Chicago

aaroncharfoos@paulhastings.com
+1.312.499.6016

Michelle A. Reed

Partner | Co-Chair, Data Privacy and Cybersecurity
Paul Hastings LLP | Dallas

michellereed@paulhastings.com
+1.972.936.7475

Paul Hastings LLP | paulhastings.com

Paul Hastings is a premier law firm providing intellectual capital and superior execution globally. Advising 50% of the Fortune 100, with 25 offices worldwide. Our Data Privacy & Cybersecurity Practice brings together industry chief counsels, privacy officers, former government officials, and regulatory and consulting experts.